TAMPEREEN YLIOPISTO

Pro gradu -tutkielma

Jukka Peltola

# Eulerin $\phi$-funktion ominaisuuksia

Informaatiotieteiden yksikkö

Matematiikka

Marraskuu 2013

Tampereen yliopisto
Informaatiotieteiden yksikkö
PELTOLA, JUKKA: Eulerin $\phi$-funktion ominaisuuksia
Pro gradu -tutkielma, 50 s.
Matematiikka
Marraskuu 2013

---

# Tiivistelmä

Eulerin $\phi$-funktio on yksi lukuteorian tunnettuja funktioita. Se kertoo jotakin lukua pienempien tämän luvun kanssa keskenään jaottomien lukujen lukumäärän. Tässä tutkielmassa käydään läpi erilaiset lukuteorian perusteet $\phi$-funktiota lähestyen. Tämän jälkeen osoitetaan funktion käytännöllisiä ja mielenkiintoisia ominaisuuksia, minkä jälkeen tutkitaan erilaisia funktion $\phi$ sisältäviä yhtälöitä.

# Sisältö

**1 Johdanto** **3**

**2 Alustavat tarkastelut** **5**

2.1 Jaollisuus ja alkuluvut . . . . . 5

2.2 Kongruenssi . . . . . 12

2.2.1 Perusominaisuuksia . . . . . 12

2.2.2 Modulaariaritmetiikan saloja . . . . . 14

2.2.3 Kiinalainen jäännöslause . . . . . 17

2.3 Aritmeettisista funktioista . . . . . 18

2.4 Möbiuksen funktio ja käänteiskaava . . . . . 20

2.5 Jakajien lukumäärä ja jakajien summa . . . . . 23

**3 Eulerin $\phi$-funktio** **26**

3.1 Määritelmä . . . . . 26

3.2 Multiplikatiivisuus . . . . . 26

3.3 Funktion arvo . . . . . 27

3.4 Eulerin $\phi$ ja kongruenssi . . . . . 33

3.5 Eulerin $\phi$ yhtälöissä ja identiteettejä . . . . . 39

**Viitteet** **50**

# 1 Johdanto

Lukuteoria on matematiikan osa-alue, joka koskee lukujen välisiä suhteita ja niiden ominaisuuksia. Lukuteoria on vanha matematiikan haara ja siihen voidaan lukea erilaisia alahaaroja. Alahaaroja ovat esimerkiksi analyyttinen lukuteoria, laskennallinen lukuteoria, jossa kehitetään uusia tietokonealgoritmeja yhä tehokkaampaan ongelmanratkaisuun, tai algebrallinen lukuteoria, jossa keskiössä ovat algebralliset luvut. C.F. Gauss totesi aikanaan, että lukuteoria on "matematiikan kuningatar", mikä on sinällään kekseliäästi sanottu, sillä lukuteorian ongelmat saattavat vaikuttaa yksinkertaisilta, mutta ovatkin mitä mutkikkaampia ja osa on vielä vailla todistusta; parhaana esimerkkinä on väite, että erittäin suuren luvun jakaminen alkutekijöihin on vaikeaa (mikä siis tietokoneiden nykyisellä teholla ja parhailla tunnetuilla tekijöidenhakualgoritmeilla pitääkin paikkansa). Tämä tutkielma uppoaa kokonaislukujen – ja siellä lisäksi alkulukujen – maailmaan.

Aritmeettiset funktiot ovat positiivisten kokonaislukujen joukossa määriteltyjä funktioita. Eulerin $\phi$-funktio on yksi aritmeettinen funktio ja lukemasi tutkielman aihe. Eulerin $\phi$-funktio kertoo jotakin lukua pienempien ja tämän luvun kanssa keskenään jaottomien lukujen lukumäärän. Funktio $\phi$ on multiplikatiivinen, mikä on yksi sen tärkeimpiä ominaisuuksia. Funktioon liittyy lukuisia jaollisuusominaisuuksia, joista yksi on yhä avoin. Osa Eulerin funktioon liittyvistä ongelmista on siis yhä vailla ratkaisua. Ks. esim. [4]. Yksi $\phi$-funktion sovellus on erinomainen julkiseen avaimeen perustuva tiedonsalausmenetelmä ja funktion avulla voi todistaa muita siihen liittymättömiäkin tuloksia.

Tutkielma rakentuu kahdesta osasta. Ensimmäisessä osassa käydään läpi tutkielman seuraamisessa vaadittavia perusteita. Alkuosio perustuu pääosin lähteisiin [6] ja [10]. Ensimmäisessä osiossa tehdään myös hieman laajempi katsaus lukuteoriaan ja käsitellään kongruenssi sekä muita aritmeettisia funktioita, kuten Möbiuksen funktio sekä funktiot, jotka laskevat jakajien

lukumäärän ja summan. Toisessa osiossa pureudutaan Eulerin $\phi$-funktioon ja osoitetaan sen lukuteoreettisessa mielessä elegantteja ominaisuuksia alkaen multiplikatiivisuudesta ja summafunktiosta. Selvitämme, miten funktion arvo voidaan laskea mille tahansa positiiviselle kokonaisluvulle ja mikä on Eulerin-Fermat'n lause. Myös muita kongruenssiominaisuuksia tarkastellaan. Aritmeettisilla funktioilla on keskinäisiä yhteyksiä ja näistä selvitämme joitakin, lähinnä funktioon $\phi$ liittyviä. Viimeisenä tutkimme erityyppisiä Eulerin $\phi$-funktion yhtälöitä, joista kysymme, millä $\phi$-funktion arvoilla ne ovat tosia, jos millään.

# 2 Alustavat tarkastelut

## 2.1 Jaollisuus ja alkuluvut

**Määritelmä 2.1** (Jaollisuus)**.** Olkoot $a, b \in \mathbb{Z}$. Luku $a$ jakaa luvun $b$, jos on olemassa sellainen $c \in \mathbb{Z}$, että $b = ac$. Merkitään

$$a \mid b.$$

Tällöin sanotaan, että *a jakaa b:n* tai *a on b:n tekijä*. Joskus sanotaan myös, että *b on a:n monikerta*. Jos $a$ ei jaa $b$:tä, merkitään $a \nmid b$.

**Määritelmä 2.2** (Alkuluku)**.** Alkuluku on sellainen lukua 1 suurempi positiivinen kokonaisluku, joka on jaollinen vain itsellään ja luvulla 1.

Jos kokonaisluku $n$ ei ole alkuluku, se on yhdistetty luku. Yhdistetyllä luvulla on vähintään kaksi tekijää $a$ ja $b$, $1 < a, b < n$.

**Esimerkki 2.1.** $2, 3, 5, 7, 11, 13$ ovat kuusi ensimmäistä alkulukua. Luku 6 on yhdistetty luku ja sen tekijät ovat 2 ja 3.

*Huomautus.* Vastikään löydettiin uusi alkuluku $2^{57\,885\,161} - 1$, joka on suurin tunnettu alkuluku. Siinä on 17 425 170 numeroa ja tarkka löytöpäivä oli 25.1.2013. [2].

**Lause 2.3.** *Jokaisella kokonaisluvulla $n > 1$ on alkulukutekijä.*

*Todistus.* Todistetaan lause käyttäen hyväksi induktiota. Jos $n = 2$, niin väitös pätee, sillä 2 on alkuluku ja itsensä tekijä. Tehdään induktio-oletus, että väitös on tosi, kun $2 \leq n \leq k$. Jos $k+1$ on alkuluku, lause on todistettu. Jos $k+1$ ei ole alkuluku, sillä on vähintään kaksi tekijää. Olkoon siis $k+1 = ab$. Tällöin $a, b \leq k$, eli induktio-oletuksen perusteella vähintään toinen on alkuluku tai molemmilla on alkulukutekijä. Täten siis luvulla $k+1$ on alkulukutekijä ja induktioperiaatteen nojalla väitös pätee jokaisella kokonaisluvulla $n > 1$. □

**Lause 2.4** (Jakoalgoritmi)**.** *Jos $a, b \in \mathbb{Z}$ ja $b > 0$, niin on olemassa sellaiset yksikäsitteiset kokonaisluvut $q$ ja $r$, että $a = bq + r$, missä $0 \leq r < b$.*

*Todistus.* Vrt. [6, s. 38]. Osoitetaan ensin yksikäsitteisyys tekemällä vastaoletus, että on olemassa myös luvut $q' \neq q$ ja $r' \neq r$, joilla $a = bq' + r', 0 \leq r' < b$. Jos nyt vähennetään luvun $a$ esitykset toisistaan, saadaan

$$\begin{aligned} bq + r - (bq' + r') &= b(q - q') + (r - r') = 0 \\ \Leftrightarrow \quad (r - r') &= b(q' - q) \end{aligned}$$

eli $b \mid r - r'$. Koska $0 \leq r < b$ ja $0 \leq r' < b$, niin $-b < r - r' < b$. Jotta tässä tilanteessa $b \mid r - r'$, pitäisi olla $r - r' = 0$ eli $r = r'$. Täten myös $q = q'$ selvästi.
Olemassaolo seuraa siitä, että joukko $S = \{a - bs : s \in \mathbb{Z}, a - bs \geq 0\}$ on epätyhjänä ei-negatiivisten lukujen joukkona hyvinjärjestetty. Tällöin joukossa on pienin alkio, joka olkoon $r = a - bq$. Joukon määrittelyn perusteella $r \geq 0$. Toisaalta $r - b = (a - bq) - b = a - b(q + 1) < 0$ eli $r < b$. Ehdot yhdistämällä saadaan $0 \leq r < b$ ja lause on todistettu. □

**Lause 2.5** (Aritmetiikan peruslause)**.** *Jokainen positiivinen kokonaisluku voidaan jakaa yksikäsitteisesti alkulukutekijöihin. Toisin sanottuna jokainen luku $n > 2$ voidaan esittää alkulukujen tulona. Saadaan luvun $n$* alkutekijähajotelma*:*

$$n = p_1 p_2 ... p_k, \quad \textit{missä } p_i \textit{ on alkuluku ja } 1 \leq i \leq k.$$

*Todistus.* Vrt. [10, s. 82]. Tehdään vastaoletus, että on olemassa pienin sellainen kokonaisluku $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l, k, l > 1$, jolle väitös ei päde. Jos olisi $p_i = q_j$ jollakin $1 \leq i \leq k$ ja $1 \leq j \leq l$, niin yhtälön voisi jakaa luvulla $p_i$. Tällöin saataisiin luvulle $\frac{n}{p_i} < n$ kaksi erillistä muotoa, mikä on ristiriita, koska $n$ on pienin tällainen luku. Oletetaan siis, että $p_1 < q_1$. Olkoon sitten $m = (q_1 - p_1)q_2 \cdots q_l = q_1 q_2 \cdots q_l - p_1 q_2 \cdots q_l = p_1 p_2 \cdots p_k - p_1 q_2 \cdots q_l = p_1(p_2 \cdots p_k - q_2 \cdots q_l)$. Nyt selvästi $m < n$ ja luvulle $m$ on kaksi erillistä alkutekijähajotelmaa. Tämä on myös ristiriita, koska $n$ on pienin tällainen luku.

Koska vastaoletus johtaa ristiriitaan, niin ei voi olla olemassa pienintä lukua, jolle ei olisi yksikäsitteistä alkutekijähajotelmaa ja väitös on todistettu. □

Alkutekijähajotelma voidaan kirjoittaa myös muodossa

$$n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}, \quad a_i \in \mathbb{Z}_+, p_i \neq p_j, \text{ kun } i \neq j,$$

jolloin on kyseessä *kanoninen* alkutekijähajotelma.

**Lause 2.6.** *Olkoon $n \in \mathbb{Z}_+$ yhdistetty luku. Tällöin sillä on alkutekijä $p_0 \leq \sqrt{n}$.*

*Todistus.* Vrt. [6, s. 71]. Olkoon $n = p_1 p_2$, $1 \leq p_1 \leq p_2 \leq n$. Jos olisi $p_1 > \sqrt{n}$, niin olisi $p_1 p_2 > \sqrt{n}\sqrt{n} = n$, mikä on ristiriita. Pitää siis olla $p_1 \leq \sqrt{n}$. Lauseen 2.3 perusteella jokaisella kokonaisluvulla $n > 1$ on alkutekijä, joten väitös seuraa ja haettu $p_0 = p_1$. □

Kokeellinen aparaatti nimeltään *Eratostheneen seula* käyttää hyväkseen lausetta 2.6. Siinä tutkitaan kaikki lukua $\sqrt{n}$ pienemmät alkuluvut ja seikka, jakavatko ne lukua $n$ pienemmät luvut. Tällä tavalla saadaan selvitettyä, mitkä ovat lukua $n$ pienemmät alkuluvut. Havainnollistetaan seulan toimintaa esimerkillä ja kysytään, mitkä ovat lukua 25 pienemmät alkuluvut?

**Esimerkki 2.2.** Nyt siis alkuluvut, jotka ovat pienempiä tai yhtäsuuria kuin $\sqrt{25} = 5$ ovat $2, 3$ ja $5$. Seulotaan ensin kaikki parilliset luvut eli $4, 6, ..., 24$ pois, koska niiden tekijänä on 2. Seulotaan sitten pois jäljelle jääneistä ne, joiden tekijänä on 3 eli $9, 15, 21$. Kaikista jäljellä olevista luvuista seulotaan vielä luvun 5 monikerrat eli 25. Jäljelle ovat jääneet luvut $7, 11, 13, 17, 23$.

**Määritelmä 2.7** (Suurin yhteinen tekijä)**.** Olkoot $a, b \in \mathbb{Z}_+$. Lukujen $a$ ja $b$ *suurin yhteinen tekijä* on suurin sellainen luku $c$, joka jakaa molemmat luvuista $a$ ja $b$. Merkitään

$$c = (a, b).$$

**Esimerkki 2.3.**

$$(8, 4) = 4, \quad (115, 110) = 5.$$

*Huomautus.* Nollalle pätevät seuraavat säännöt

$$(0,0) = 0 \quad \text{ja} \quad (a,0) = a, \quad \forall a \in \mathbb{Z}.$$

**Määritelmä 2.8** (Keskenään jaottomat luvut)**.** Luvut $a$ ja $b$ ovat *keskenään jaottomat*, jos

$$(a,b) = 1.$$

**Lause 2.9.** *Olkoon $(a,b) = d$ ja ainakin toinen luvuista $a$ ja $b$ poiketkoon nollasta. Tällöin $d$ on pienin niistä luvuista, jotka voidaan esittää lukujen $a$ ja $b$ positiivisena lineaarikombinaationa.*

*Todistus.* Vrt. [10, s. 59]. Olkoon

$$T = \{ax + by : x, y \in \mathbb{Z} \text{ ja } ax + by > 0\}.$$

Hyvinjärjestysperiaatteen mukaan joukossa $T$ on pienin alkio, joka olkoon $e = ak + bl$. Jakoalgoritmin nojalla on olemassa sellaiset $q$ ja $r$, että $a = eq + r, 0 \leq r < e$. Nyt siis

$$r = a - eq = a - (ak + bl)q = a(1 - kq) + b(-lq)$$

eli, jos $r \neq 0$, niin $r$ on lukujen $a$ ja $b$ lineaarikombinaatio ja joukossa $T$. Koska $r$ on pienempi kuin joukon $T$ pienin alkio, pitää kuitenkin olla $r = 0$. Tämä siis tarkoittaa, että $a = eq$ eli $e \mid a$. Vastaavasti voidaan päätellä, että $e \mid b$. Koska $e$ jakaa molemmat luvuista $a$ ja $b$ ja $d = (a,b)$ on oltava $e \leq d$. Lisäksi, koska $d \mid a$ ja $d \mid b$, niin $d \mid ak + bk = e$ eli $d \leq e$. Siis $d = e$ on joukon $T$ pienin alkio. □

**Seuraus 2.10.** *Olkoot $a, b \in \mathbb{Z}$ ja $(a,b) = d$. Tällöin on olemassa sellaiset $x, y \in \mathbb{Z}$, että $d = ax + by$.*

**Lause 2.11.** *Olkoot $a, b \in \mathbb{Z}$. Tällöin $(a,b) = 1$, jos ja vain jos on olemassa sellaiset $x, y \in \mathbb{Z}$, että $ax + by = 1$.*

*Todistus.* Lause seuraa suoraan edellisestä. □

Todistetaan seuraavaksi joitakin jaollisuuteen liittyviä lauseita. Ks. esim. [6].

**Lause 2.12.** *Olkoot $a, b, c \in \mathbb{Z}$ sekä $a \mid b$ ja $b \mid c$. Tällöin $a \mid c$.*

*Todistus.* Oletuksen perusteella on olemassa sellaiset kokonaisluvut $k$ ja $l$, että $b = ak$ ja $c = bl$. Nyt siis $c = (ak)l = a(kl)$ eli $a \mid c$. □

**Lause 2.13.** *Olkoot $a, b, c, m, n \in \mathbb{Z}$ sekä $c \mid a$ ja $c \mid b$. Tällöin $c \mid ma + nb$.*

*Todistus.* Oletuksen perusteella on olemassa sellaiset kokonaisluvut $k$ ja $l$, että $a = kc$ ja $b = lc$. Nyt

$$ma + nb = mkc + nlc = (mk + nl)c$$

eli $c \mid ma + nb$. □

**Lause 2.14.** *Olkoot $a, b \in \mathbb{Z}_+$ sekä $a \mid b$. Tällöin $a \leq b$.*

*Todistus.* Oletuksen perusteella on olemassa sellainen kokonaisluku $k > 0$, että $b = ak$. Todistetaan lause induktiolla. Oletetaan siis ensin, että $k = 1$. Tällöin $b = a \geq a$. Oletetaan sitten, että väite on tosi, kun $k = n$ eli $b = an \geq a$. Jos $k = n+1$, niin $b = a(n+1) = an + a \geq a + a \geq a$. Induktio-oletuksella perustellaan toiseksi viimeinen erisuuruus ja viimeinen on itsestään selvää. Tulos seuraa induktioperiaatteen nojalla. □

**Lause 2.15.** *Olkoot $a, b, c \in \mathbb{Z}_+$ sekä $(a, b) = 1$ ja $a \mid bc$. Tällöin $a \mid c$.*

*Todistus.* Koska $(a, b) = 1$, niin lause 2.11 osaa kertoa, että on olemassa sellaiset $x, y \in \mathbb{Z}$, että $ax + by = 1$. Kerrotaan yhtälöön $c$, jolloin saadaan $axc + byc = c$. Koska $a \mid a$ sekä $a \mid bc$, niin lauseen 2.13 nojalla $a \mid a(xc) + bc(y) = c$. □

**Lause 2.16.** *Olkoot $a, b, c \in \mathbb{Z}_+$ sekä $(a, b) = 1$, $a \mid c$ ja $b \mid c$. Tällöin $ab \mid c$.*

*Todistus.* Oletuksen perusteella on olemassa sellaiset $k, l \in \mathbb{Z}$, että $ak = bl = c$. Koska $a$ ja $b$ ovat keskenään jaottomia, niin lauseen 2.9 perusteella

on olemassa sellaiset $x, y \in \mathbb{Z}$, että $ax + by = 1$. Kerrotaan taas $c$ yhtälöön ja saadaan

$$c = axc + byc = ax(bl) + by(ak) = ab(xl) + ab(yk) = ab(xl + yk)$$

eli $ab \mid c$. □

Todistetaan seuraavaksi lause, jonka avulla on mahdollista löytää kahden luvun suurin yhteinen tekijä. Siinä käytetään toistuvasti lauseessa 2.4 esiteltyä jakoalgoritmia ja lause kulkee nimellä *Eukleideen algoritmi*. Todistetaan vielä ennen varsinaisen Eukleideen algoritmin todistusta tarpeellinen apulause. [6, s. 103].

**Apulause 2.17.** *Olkoot $a, b, q, r \in \mathbb{Z}$ ja $a = bq + r$. Tällöin $(a, b) = (b, r)$.*

*Todistus.* Merkitään $(a, b) = k$ ja $(b, r) = l$. Osoitetaan, että $k \leq l$ ja $l \leq k$ eli $k = l$. Nyt siis $k \mid a$ ja $k \mid b$ eli on olemassa sellaiset kokonaisluvut $d$ ja $e$, että $a = dk$ ja $b = ek$. Saadaan

$$dk = ekq + r \Leftrightarrow r = dk - ekq = (d - eq)k$$

eli $k \mid r$. Koska $(b, r) = l$, niin on oltava $k \leq l$. Toisaalta $l \mid b$ ja $l \mid r$, joten on olemassa sellaiset kokonaisluvut $f$ ja $g$, että $b = fl$ ja $r = gl$. Saadaan

$$a = flq + gl = (fq + g)l$$

eli $l \mid a$. Edellä todettiin, että myös $l \mid b$, mutta koska $(a, b) = k$, niin pitää olla $l \leq k$. Pitää siis paikkansa, että $(a, b) = (b, r)$. □

**Lause 2.18** (Eukleideen algoritmi)**.** *Olkoot $a, b \in \mathbb{Z}$ ja $0 < b \leq a$. Olkoot lisäksi $q_1, q_2, ..., q_{n+1}$ osamääriä ja $r_1, r_2, ..., r_{n+1}$ jäännöksiä, jotka saadaan*

*jakoalgoritmia käyttämällä seuraavasti*

$$\begin{aligned} a &= bq_1 + r_1, \quad 0 \leq r_1 < b, \\ b &= r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1, \\ r_1 &= r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2, \\ &\dots \\ r_{n-2} &= r_{n-1} q_n + r_n, \quad 0 \leq r_n < r_{n-1} \text{ ja} \\ r_{n-1} &= r_n q_{n+1} + r_{n+1} \end{aligned}$$

*ja* $r_{n+1} = 0$. *Tällöin* $(a, b) = r_n$.

*Todistus.* Sovelletaan apulausetta 2.17. Saadaan

$$(a, b) = (b, r_1) = (r_1, r_2) = ... = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = (r_n, 0) = r_n.$$

Siis $(a, b) = r_n$. □

**Lause 2.19.** *Olkoot* $d, m, n \in \mathbb{Z}_+$ *sekä* $(m, n) = 1$. *Jos* $d \mid mn$, *niin on olemassa sellaiset yksikäsitteiset* $d_1, d_2 \in \mathbb{Z}_+$, *että* $d_1 \mid m, d_2 \mid n$ *ja* $d = d_1 d_2$. *Toisaalta myös, jos* $d_1 \mid m$ *ja* $d_2 \mid n$, *niin* $d = d_1 d_2 \mid mn$.

*Todistus.* Vrt. [6, s. 117]. Olkoot $m = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}$ ja $n = q_1^{n_1} q_2^{n_2} \cdots q_t^{n_t}$. Kaikki $p_1, p_2, ..., p_s$ ovat keskenään jaottomia lukujen $q_1, q_2, ..., q_t$ kanssa, koska $(m, n) = 1$. Tällöin siis

$$mn = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s} q_1^{n_1} q_2^{n_2} \cdots q_t^{n_t}.$$

Oletetaan sitten, että $d \mid mn$, jolloin saadaan

$$d = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} q_1^{f_1} q_2^{f_2} \cdots q_t^{f_t},$$

missä $0 \leq e_i \leq m_i$, kaikilla $i = 1, 2, ..., s$ ja $0 \leq f_j \leq n_j$, kaikilla $j = 1, 2, ..., t$. Nyt oletetaan lisäksi, että $d_1 = (d, m)$ ja $d_2 = (d, n)$, jolloin

$$\begin{aligned} d_1 &= p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} \\ d_2 &= q_1^{f_1} q_2^{f_2} \cdots q_t^{f_t}. \end{aligned}$$

Selvästi $d = d_1 d_2$ ja koska $(m, n) = 1$, niin $(d_1, d_2) = 1$. Löydetyt luvut $d_1$ ja $d_2$ ovat myös yksikäsitteiset, sillä lukujen $m$ ja $n$ alkutekijähajotelmat ovat yksikäsitteiset sekä $d_1$ ja $d_2$ käsittävät kaikki luvun $d$ alkulukupotenssit. Edelleen $d_1$ käsittää vain kaikki ne alkulukupotenssit, jotka ovat luvun $m$ tekijöitä ja vastaavasti $d_2$ käsittää potenssit, jotka ovat luvun $n$ tekijöitä. Osoitetaan väitös vielä toiseen suuntaan.
Oletetaan, että $d_1 \mid m$ ja $d_2 \mid n$. Tällöin

$$\begin{aligned} d_1 =& p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}, \quad \text{missä } 0 \leq e_i \leq m_i, \text{ kaikilla } i = 1, 2, ..., s \\ d_2 =& q_1^{f_1} q_2^{f_2} \cdots q_t^{f_t}, \quad \text{missä } 0 \leq f_j \leq n_j, \text{ kaikilla } j = 1, 2, ..., t. \end{aligned}$$

Selvästi $d = d_1 d_2 = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} q_1^{f_1} q_2^{f_2} \cdots q_t^{f_t}$ jakaa luvun $mn$, koska minkään alkutekijähajotelmassa esiintyvän alkuluvun potenssi ei ylity. □

## 2.2 Kongruenssi

Kongruenssin käsite on lukuteoriassa fundamentaali. Se mahdollistaa aritmetiikan kaltaisen ongelmanratkaisun jaollisuuteen liittyvissä ongelmissa. Tarkastellaan kongruenssin käsitettä seuraavaksi hieman tarkemmin lähteitä [6] ja [10] seuraillen.

### 2.2.1 Perusominaisuuksia

**Määritelmä 2.20** (Kongruenssi)**.** Olkoon $n > 1$. Luvut $a$ ja $b$ ovat *kongruentteja modulo* $n$, jos $n \mid a - b$. Merkitään

$$a \equiv b \pmod{n}.$$

**Esimerkki 2.4.** Suuri osa ihmisistä käyttää tietoisesti tai tiedostamattaan kongruenssia arkielämässään. Nimittäin kello tai viikkokalenteri ovat oivia esimerkkjä käytännön kongruenssista. Kun kello on yhdeksäntoista, sen voidaan sanoa olevan seitsemän: $19 \equiv 7 \pmod{12}$. Numeroidaan viikonpäivät maanantaista sunnuntaihin yhdestä seitsemään. Yhdeksäntoista päivää maanantaista on lauantai: $1 + 19 = 20 \equiv 6 \pmod{7}$.

**Lause 2.21.** *Olkoot $a, b \in \mathbb{Z}$ sekä $a \equiv b \pmod{n}$. Tällöin on olemassa sellainen $k \in \mathbb{Z}$, että $a = b + kn$. Vastaavasti, jos $a = b + kn$, niin $a \equiv b \pmod{n}$.*

*Todistus.* Oletetaan siis ensin, että $a \equiv b \pmod{n}$. Tällöin $n \mid a - b$, mikä taas tarkoittaa, että on olemassa sellainen $k$, että $kn = a - b$, mistä seuraa, että $a = b + kn$.
Oletetaan sitten, että $a = b + kn$. Tapaus menee vastaavasti kuin edellinen, mutta käänteisesti eli oletuksen perusteella $kn = a - b$, mikä tarkoittaa, että $n \mid a - b$ eli $a \equiv b \pmod{n}$. □

**Lause 2.22.** *Olkoon $n \in \mathbb{Z}_+$. Kongruenssi modulo $n$ on kokonaislukujen joukossa määritelty ekvivalenssirelaatio eli kongruenssilla modulo $n$ on seuraavat ominaisuudet:*

(i) *Refleksiivisyys; Jos $a \in \mathbb{Z}$, niin $a \equiv a \pmod{n}$.*

(ii) *Symmetrisyys; Jos $a, b \in \mathbb{Z}$ ja $a \equiv b \pmod{n}$, niin $b \equiv a \pmod{n}$.*

(iii) *Transitiivisuus; Jos $a, b, c \in \mathbb{Z}$ sekä $a \equiv b \pmod{n}$ ja $b \equiv c \pmod{n}$, niin $a \equiv c \pmod{n}$.*

*Todistus.*

(i) Kaikilla luvuilla $a \in \mathbb{Z}$ pätee $a = a + 0 \cdot n$ eli $n \mid a - a$. Siis $a \equiv a \pmod{n}$.

(ii) Nyt on olemassa sellainen $k \in \mathbb{Z}$, että $a = b + kn$ eli $b = a + (-k)n$. Siis $b \equiv a \pmod{n}$.

(iii) Nyt on olemassa sellaiset $k, l \in \mathbb{Z}$, että $a = b + kn$ ja $b = c + ln$, mistä saadaan $a = c + ln + kn = c + (l + k)n$. Siis $a \equiv c \pmod{n}$.

□

Ekvivalenssirelaatio jakaa joukon ekvivalenssiluokkiin. Huomataan, että lauseen 2.22 perusteella kongruenssi modulo $n$ jakaa kokonaisluvut ekvivalenssiluokkiin, joita on yhteensä $n$ kappaletta. Tässä yhteydessä ekvivalenssiluokkia kutsutaan *jäännösluokiksi modulo n*.

Esitellään vielä ennen kongruenssin laskusääntöjä lineaarinen kongruenssiyhtälö sekä kongruenssin käänteisluvun käsite. Kongruenssi, joka on muotoa

$$ax \equiv b \pmod{n},$$

on *yhden muuttujan lineaarinen kongruenssiyhtälö*. Jokainen jäännössysteemin modulo $n$ alkio on kongruenssiyhtälön ratkaisu, jos yksikin sen alkioista on ratkaisu.

**Lause 2.23.** *Olkoot $a, b, n \in \mathbb{Z}, n > 0$ ja $(a, n) = d$. Jos $d \nmid b$, niin kongruenssiyhtälöllä $ax \equiv b \pmod{n}$ ei ole ratkaisua. Jos sen sijaan $d \mid b$, niin kongruenssiyhtälöllä $ax \equiv b \pmod{n}$ on täsmälleen $d$ ratkaisua modulo $n$.*

*Todistus.* Ks. [6, s. 158]. □

**Seuraus 2.24.** *Olkoot $a, b, n \in \mathbb{Z}, n > 0$ ja $(a, n) = 1$. Tällöin kongruenssiyhtälöllä $ax \equiv b \pmod{n}$ on yksikäsitteinen ratkaisu modulo $n$.*

*Todistus.* Väite seuraa suoraan lauseesta 2.23. □

Jos kongruenssiyhtälössä $ax \equiv b \pmod{n}$, jolla on yksikäsitteinen ratkaisu modulo $n$, on $b = 1$, niin kyseessä on seuraava erikoistapaus.

**Määritelmä 2.25.** Olkoon $a \in \mathbb{Z}$ ja $(a, n) = 1$. Kongruenssiyhtälön $ax \equiv 1 \pmod{n}$ ratkaisu $x \in \mathbb{Z}$ on luvun *$a$ käänteisluku modulo $n$*.

### 2.2.2 Modulaariaritmetiikan saloja

Kongruenssiyhtälö muistuttaa aritmeettista yhtälöä. Yhteys ei lopu ulkoiseen olemukseen, nimittäin kongruenssiyhtälöä voi operoida puolittain aritmeettisilla operaatioilla. Tätä kutsutaan *modulaariaritmetiikaksi*. Osoitetaan seuraavaksi, että kongruenssi säilyy yhteen-, vähennys- ja kertolaskussa sekä potenssiin korotuksessa.

**Lause 2.26.** *Olkoot* $a, b, c, n, s \in \mathbb{Z}$ *ja* $n, s > 0$ *sekä* $a \equiv b \pmod{n}$. *Tällöin*

(i) $a \pm c \equiv b \pm c \pmod{n}$,

(ii) $ac \equiv bc \pmod{n}$ *ja*

(iii) $a^s \equiv b^s \pmod{n}$.

*Todistus.*

(i) Oletuksen perusteella on olemassa sellainen $k \in \mathbb{Z}$, että $a = b + kn$ eli $n \mid a - b = a + c - (b + c)$. Tästä saadaan $a + c = b + c + kn$, joten $a + c \equiv b + c \pmod{n}$. Vähennyslaskun tapaus on täysin vastaava.

(ii) Kertolaskun tapauksessa analogia on vastaavahko, nimittäin $ac - bc = c(a-b)$. Edellä on todettu, että $n \mid a-b$, joten myös $n \mid c(a-b) = ac-bc$ eli $ac \equiv bc \pmod{n}$.

(iii) Nyt $a^s - b^s = (a-b)(a^{s-1} + a^{s-2}b + ... + ab^{s-2} + b^{s-1})$ eli $a - b \mid a^s - b^s$. Kuten on mainittu, oletuksen mukaan $n \mid a - b$, joten lauseen 2.12 perusteella $n \mid a^s - b^s$ eli $a^s = b^s + kn$ eli $a^s \equiv b^s \pmod{n}$.

□

Todistetaan jatkoa silmällä pitäen vielä seuraava kertolaskuun liittyvä lause [10, s. 152].

**Lause 2.27.** *Jos* $a_i \equiv b_i \pmod{n}$, *kaikilla* $1 \leq i \leq s$, *niin*

$$\prod_{i=1}^{s} a_i \equiv \prod_{i=1}^{s} b_i \pmod{n}.$$

*Todistus.* Todistetaan lause induktiolla luvun $s$ suhteen. Olkoon $s = 1$. Tällöin

$$a_1 \equiv b_1 \pmod{n},$$

mikä on tosi, sillä $a_i \equiv b_i \pmod{n}$, kaikilla $1 \leq i \leq s$. Tehdään sitten induktio-oletus, että väitös pätee, kun $s = k - 1$ eli

$$\prod_{i=1}^{k-1} a_i \equiv \prod_{i=1}^{k-1} b_i \pmod{n},$$

mikä siis tarkoittaa, että

$$n \mid \prod_{i=1}^{k-1} a_i - \prod_{i=1}^{k-1} b_i.$$

Oletetaan sitten, että $s = k$. Oletuksen perusteella $n \mid a_k - b_k$, joten lauseen 2.13 perusteella

$$\begin{aligned} n \mid \prod_{i=1}^{k-1} a_i \cdot (a_k - b_k) + b_k \cdot \left( \prod_{i=1}^{k-1} a_i - \prod_{i=1}^{k-1} b_i \right) &= \prod_{i=1}^{k} a_i - b_k \cdot \prod_{i=1}^{k-1} a_i + b_k \prod_{i=1}^{k-1} a_i - \prod_{i=1}^{k} b_i \\ &= \prod_{i=1}^{k} a_i - \prod_{i=1}^{k} b_i \end{aligned}$$

eli $\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \pmod{n}$, joten lause on tosi induktioperiaatteen nojalla. □

Kongruenssin jakaminen ei ole aivan yhtä suoraviivaista kuin kertominen tai yhteenlasku. Esimerkiksi $2 \cdot 2 = 4 \equiv 10 = 2 \cdot 5 \pmod{6}$ ei ole jaettavissa kahdella kertolaskun tapaan, vaikka siltä näin ensialkuun saattaakin näyttää. Nimittäin $2 \not\equiv 5 \pmod{6}$. Osoitetaan seuraavaksi, että kongruenssi voidaan kuitenkin jakaa – tarkemmin ottaen kyse on yhteisen tekijän eliminoinnista – tietyissä tilanteissa [6, s. 149].

**Lause 2.28.** *Olkoot $a, b, c, n \in \mathbb{Z}$ ja $n > 0$. Jos $(c, n) = d$ ja $ac \equiv bc \pmod{n}$, niin $a \equiv b \pmod{\frac{n}{d}}$.*

*Todistus.* Oletetaan, että $ac \equiv bc \pmod{n}$. Tällöin $n \mid ac - bc = c(a - b)$, joten on olemassa sellainen kokonaisluku $k$, että $kn = c(a - b)$. Kun jaetaan puolittain kokonaisluvulla $d$, saadaan

$$k\frac{n}{d} = \frac{c}{d}(a - b).$$

Koska $(c, n) = d$, niin $(\frac{c}{d}, \frac{n}{d}) = 1$, joten lauseen 2.15 perusteella $\frac{n}{d} | a - b$ eli $a \equiv b \pmod{\frac{n}{d}}$ ja lause on todistettu. □

**Seuraus 2.29.** *Olkoon $ac \equiv bc \pmod{n}$ ja $(c, n) = 1$. Tällöin $a \equiv b \pmod{n}$.*

**Esimerkki 2.5.** Jaetaan edellinen esimerkki kahdella. Nyt $2 \cdot 2 = 4 \equiv 10 = 2 \cdot 5 \pmod 6$ ja $(2, 6) = 2$, joten $2 \equiv 5 \pmod 3$. Jos kongruenssiyhtälön molempien puolien yhteinen tekijä on jaoton modulin kanssa, voidaan sillä jakaa, kuten seurauslause 2.29 toteaa: $2 \cdot 2 = 4 \equiv 18 = 2 \cdot 9 \pmod 7$ ja koska $(2, 7) = 1$, niin $2 \equiv 9 \pmod 7$.

**Määritelmä 2.30.** Kokonaislukujen joukko on *täydellinen jäännössysteemi modulo $n$*, jos jokainen kokonaisluku on kongruentti täsmälleen yhden tämän joukon luvun kanssa modulo $n$.

**Määritelmä 2.31.** Lukujoukko $\{0, 1, 2, ..., n-1\}$ on *pienimpien ei-negatiivisten jäännösten systeemi modulo $n$.*

**Määritelmä 2.32.** Lukumäärältään suurin sellainen täydellisen jäännössysteemin modulo $n$ osajoukko, jonka luvut ovat jaottomia luvun $n$ kanssa, on *supistettu jäännössysteemi modulo $n$.*

Myöhemmin tutkielmassa selviää, montako alkiota supistetussa jäännössysteemissä modulo $n$ on.

### 2.2.3 Kiinalainen jäännöslause

Ennen aritmeettisten funktioiden esittelyä, todistetaan vielä yksi kongruensseihin liittyvä tulos. Kyseessä on lineaarisen kongruenssiyhtälöryhmän ratkaiseminen. Jokaisessa kongruenssiyhtälössä moduli on eri ja kyseessä on *kiinalainen jäännöslause.*

**Lause 2.33** (Kiinalainen jäännöslause)**.** *Olkoot $m_1, m_2, ..., m_k \in \mathbb{Z}$ pareittain keskenään jaottomia. Tällöin kongruenssiyhtälöryhmällä*

$$x \equiv a_i \pmod{m_i}, \qquad \textit{missä } 1 \leq i \leq k$$

*on yksikäsitteinen ratkaisu modulo $M = \prod_{i=1}^{k} m_i$.*

*Todistus.* Vrt. [10, s. 173]. Olkoon $M_j = \frac{M}{m_j}$, missä $1 \leq j \leq k$ ja $M = \prod_{i=1}^{k} m_i$. Nyt koska $m_1, m_2, ..., m_k$ ovat pareittain keskenään jaottomia, niin

$m_l \mid M_j$ ja $(m_j, m_l) = 1$, kaikilla $l \neq j$. Kun olemme määritelleet luvun $M_j$ tällä tavalla, niin $(m_j, M_j) = 1$, jolloin kongruenssiyhtälöllä $M_j y \equiv 1 \pmod{m_j}$ on seurauslauseen 2.24 perusteella yksikäsitteinen ratkaisu $y$ eli käänteisluku $b_j$ modulo $m_j$. Siis jokaiselle $j$ on olemassa sellainen $b_j$, että $M_j b_j \equiv 1 \pmod{m_j}$. Muodostetaan sitten summa $x \equiv \sum_{j=1}^{k} M_j b_j a_j \pmod{M}$. Summattavissa $M_j b_j a_j \equiv a_j \pmod{m_j}$, koska $M_j b_j \equiv 1 \pmod{m_j}$, ja $M_j \equiv 0 \pmod{m_l}$, kun $j \neq l$. Tällöin siis $x \equiv a_j \pmod{m_j}$. Siis $x$ on kongruenssiyhtälöryhmän ratkaisu. Yksikäsitteisyyden modulo $M$ osoitamme olettamalla ensin, että $x_0$ ja $x_1$ ovat erilliset kongruenssiyhtälöryhmän ratkaisut, jolloin saadaan

$$x_0 \equiv x_1 \equiv a_j \pmod{m_j}, \qquad \text{kaikilla } 1 \leq j \leq k.$$

Tällöin on olemassa sellaiset $k_0, k_1 \in \mathbb{Z}$, että $x_0 = a_j + k_0 m_j$ ja $x_1 = a_j + k_1 m_j$ ja yhtälöt yhdistämällä saadaan

$$x_1 = x_0 - k_0 m_j + k_1 m_j \Leftrightarrow x_1 - x_0 = (k_1 - k_0) m_j$$

eli $m_j \mid x_1 - x_0$ kaikilla $1 \leq j \leq k$. Koska jokainen $m_j \mid x_1 - x_0$, niin myös $M \mid x_1 - x_0$, joten $x_0 \equiv x_1 \pmod{M}$ ja myös yksikäsitteisyys on osoitettu. □

## 2.3 Aritmeettisista funktioista

Aritmeettiset funktiot on määritelty kokonaislukujen joukossa. Eulerin $\phi$-funktio on eräs aritmeettinen funktio. Toinen keskeinen funktio, nimittäin Möbiuksen funktio, esitellään myös. Se osoittautuu oivaksi avuksi myöhemmin, kun osoitamme $\phi$-funktioon liittyviä tuloksia. Lisäksi lyhyen esittelyn saavat sellaiset aritmeettiset funktiot kuin jakajien lukumäärä sekä jakajien summa. Kokonaisuus tai sen osia löytyy useammastakin lähteestä, mutta notaatiot ja todistusten analogia noudattelevat lähdettä [6].

**Määritelmä 2.34** (Aritmeettinen funktio)**.** Funktio, jonka määrittelyjoukko on $\mathbb{Z}_+$, on *aritmeettinen funktio.*

**Määritelmä 2.35** (Multiplikatiivinen funktio)**.** Aritmeettinen funktio $f$ on *multiplikatiivinen*, jos

$$f(mn) = f(m)f(n), \quad \text{kun } (m,n) = 1,$$

ja *täydellisesti multiplikatiivinen*, jos

$$f(mn) = f(m)f(n), \quad \forall m, n \in \mathbb{Z}_+.$$

**Esimerkki 2.6.** Vakiofunktio $f(n) = 1$ on täydellisesti multiplikatiivinen.

Jos $f$ on aritmeettinen funktio, niin

$$F(n) = \sum_{d|n} f(d)$$

on sen summafunktio. Ennen kuin osoitetaan, että multiplikatiivisen funktion summafunktio on multiplikatiivinen, tarkastellaan sitä hieman tarkemmin lyhyen esimerkin kautta.

**Esimerkki 2.7.** Olkoon $f(n) = n$. Sen summafunktio on tällöin $F(n) = \sum_{d|n} f(d) = \sum_{d|n} d$. Lasketaan summa, kun $n = 4$:

$$F(4) = f(1) + f(2) + f(4) = 1 + 2 + 4 = 7.$$

**Lause 2.36.** *Jos $f$ on multiplikatiivinen, niin on myös*

$$F(n) = \sum_{d|n} f(d).$$

*Todistus.* Olkoot $m$ ja $n$ keskenään jaottomia positiivisia kokonaislukuja. Tällöin

$$F(mn) = \sum_{d|mn} f(d).$$

Koska $(m,n) = 1$, niin lauseen 2.19 perusteella on olemassa sellaiset keskenään jaottomat luvut $a$ ja $b$, että $a \mid m$, $b \mid n$ ja $ab = d$. Nyt siis

$$F(mn) = \sum_{a|m, b|n} f(ab).$$

Koska $f$ on multiplikatiivinen, niin

$$F(mn) = \sum_{a|m,b|n} f(ab) = \sum_{a|m,b|n} f(a)f(b) = \sum_{a|m} f(a) \sum_{b|n} f(b) = F(m)F(n).$$

□

**Lause 2.37.** *Jos $f$ ja $g$ ovat multiplikatiivisia, niin on myös*

$$F(n) = \sum_{d|n} f(d)g(\frac{n}{d}).$$

*Todistus.* Jos $m$ ja $n$ ovat keskenään jaottomia, niin $d \mid mn$, jos ja vain jos $d = kl$, missä $k \mid m$ ja $l \mid n$ sekä $(k, l) = 1$ ja $(\frac{m}{k}, \frac{n}{l}) = 1$. Täten

$$\begin{aligned} F(mn) &= \sum_{d|mn} f(d)g(\frac{mn}{d}) = \sum_{d|k} \sum_{d|l} f(kl)g(\frac{mn}{kl}) \\ &= \sum_{d|k} \sum_{d|l} f(k)f(l)g(\frac{m}{k})g(\frac{n}{l}) \\ &= \sum_{d|k} f(k)g(\frac{m}{k}) \sum_{d|l} f(l)g(\frac{n}{l}) = F(m)F(n). \end{aligned}$$

□

*Huomautus.* Kun merkitään lauseen 2.37 summafunktiota $F = f * g$, niin muotoa sanotaan myös *Dirichlet'n konvoluutioksi.*

## 2.4 Möbiuksen funktio ja käänteiskaava

Möbiuksen funktio on käyttökelpoinen apu Eulerin $\phi$-funktion osoittamisessa multiplikatiiviseksi.

**Määritelmä 2.38** (Möbiuksen funktio)**.** Möbiuksen funktio $\mu(n)$ määritellään seuraavasti

$$\mu(n) = \begin{cases} 1, & \text{jos } n = 1, \\ (-1)^k, & \text{jos } n = p_1 p_2 ... p_k \text{ , missä } p_i \neq p_j \text{ , kun } i \neq j, \\ 0, & \text{muulloin.} \end{cases}$$

Osoitetaan ensin, että Möbiuksen funktio on multiplikatiivinen.

**Lause 2.39.** *Möbiuksen funktio on multiplikatiivinen.*

*Todistus.* Olkoon $(m, n) = 1$. Osoitetaan multiplikatiivisuus kolmessa osassa määritelmän osoittamassa järjestyksessä. Oletetaan siis ensin, että $m = 1$. Tällöin

$$\mu(mn) = \mu(n) = \mu(m)\mu(n).$$

Viimeinen kohta pätee, koska $\mu(m) = 1$. Tapaus $n = 1$ menee vastaavasti. Oletetaan seuraavaksi, että $m = p_1 p_2 ... p_k$, missä $p_i \neq p_j$, kun $i \neq j$ ja $n = q_1 q_2 ... q_l$, missä $q_i \neq q_j$, kun $i \neq j$. Nyt

$$\mu(m)\mu(n) = (-1)^k(-1)^l = (-1)^{k+l}.$$

Koska $(m, n) = 1$, niin $q_i \neq p_j, \forall i, j$. Tällöin

$$\mu(mn) = (-1)^{k+l},$$

mikä todistaa tapauksen. Muissa tapauksissa $\mu(m) = 0$ tai $\mu(n) = 0$ eli myös $\mu(mn) = 0 = \mu(m)\mu(n)$ ja lause on todistettu. □

**Lause 2.40.** *Möbiuksen funktion summafunktio on*

$$F(n) = \sum_{d|n} \mu(d) = \begin{cases} 1 & , \quad jos\ n = 1, \\ 0 & , \quad jos\ n > 1. \end{cases}$$

*Todistus.* Oletetaan ensin, että $n = 1$. Tällöin

$$F(n) = \sum_{d|n} \mu(d) = \mu(1) = 1$$

ja ensimmäinen vaihe on todistettu.
Oletetaan sitten, että $n > 1$. Koska Möbiuksen funktio on multiplikatiivinen, niin lauseen 2.36 nojalla myös $F(n)$ on multiplikatiivinen. Lisäksi lauseen yhtälön oikean puolen funktio on multiplikatiivinen. Tällöin riittää tarkastella tapausta, että $n = p^k$, missä $k$ on mikä tahansa positiivinen kokonaisluku. Olkoon siis $n = p^k$, missä ensin $k = 1$. Silloin

$$F(n) = F(p) = \sum_{d|p} \mu(d) = \mu(1) + \mu(p) = 1 + (-1) = 0.$$

Olkoon sitten $n = p^k$, missä $k > 1$. Silloin

$$\begin{aligned} F(n) = F(p^k) &= \sum_{d|p^k} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + ... + \mu(p^k) \\ &= 1 + (-1) + 0 + 0 + ... + 0 = 0. \end{aligned}$$

Kummassakin tapauksessa lauseen yhtälön oikean puolen funktio on myös nolla, sillä $n > 1$. Näin myös toinen vaihe ja täten koko lause on todistettu. □

**Lause 2.41** (Möbiuksen käänteiskaava)**.** *Olkoon $f$ aritmeettinen funktio ja $F(n) = \sum_{d|n} f(d), \forall n \in \mathbb{Z}_+$. Tällöin*

$$f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d}), \quad \forall n \in \mathbb{Z}_+.$$

*Todistus.* Nyt

$$\sum_{d|n} \mu(d) F(\frac{n}{d}) = \sum_{d|n} \mu(d) \sum_{k|\frac{n}{d}} f(k) = \sum_{d|n} \sum_{k|\frac{n}{d}} \mu(d) f(k).$$

Koska $d \mid n$ ja $k \mid \frac{n}{d}$, niin on olemassa sellainen $a$, että $\frac{n}{d} = ak$. Tästä saadaan $n = adk$ ja $\frac{n}{k} = ad$ eli $k \mid n$ ja $d \mid \frac{n}{k}$. Voidaan siis korvata pari $d \mid n$ ja $k \mid \frac{n}{d}$ parilla $k \mid n$ ja $d \mid \frac{n}{k}$, jolloin kääntämällä samalla summausjärjestyksen saadaan

$$\sum_{k|n} \sum_{d|\frac{n}{k}} f(k)\mu(d) = \sum_{k|n} f(k) \sum_{d|\frac{n}{k}} \mu(d) = f(n) \cdot 1 = f(n).$$

Viimeinen kohta seuraa siitä, että $\sum_{d|\frac{n}{k}} \mu(d) = 0$, kun $\frac{n}{k} > 1$, joten pitää olla $\frac{n}{k} = 1$ eli $n = k$, jolloin $\sum_{d|\frac{n}{k}} \mu(d) = 1$ ja $\sum_{k|n} f(k) = f(n)$. □

Möbiuksen käänteiskaavalla voidaan osoittaa lauseen 2.36 pätevän myös toiseen suuntaan.

**Lause 2.42.** *Jos $F$ on multiplikatiivinen ja $F(n) = \sum_{d|n} f(d)$, niin myös $f$ on multiplikatiivinen.*

*Todistus.* Olkoon $(m,n)=1$. Möbiuksen käänteiskaavan nojalla voidaan kirjoittaa

$$f(mn)=\sum_{d|mn}\mu(d)F(\frac{mn}{d}),$$

missä $\mu$ ja $F$ ovat multiplikatiivisia. Tällöin lauseen 2.37 perusteella myös $\sum_{d|n}\mu(d)F(\frac{n}{d})$ on multiplikatiivinen, siis

$$\sum_{d|mn}\mu(d)F(\frac{mn}{d})=\sum_{d|m}\mu(d)F(\frac{m}{d})\sum_{d|n}\mu(d)F(\frac{n}{d})=f(m)f(n).$$

□

## 2.5 Jakajien lukumäärä ja jakajien summa

Eulerin $\phi$-funktiolle löytyy monta yhteyttä jakajien lukumäärä - ja jakajien summa -funktioihin, joten esitellään ne myöhempiä tuloksia varten tässä vaiheessa. Aloitetaan funktioiden määritelmillä.

**Määritelmä 2.43** (Jakajien lukumäärä)**.** Kaikille $n\in\mathbb{Z}_+$

$$\tau(n)=|\{d\in\mathbb{Z}_+ : d\mid n\}|=\sum_{d|n}1.$$

**Määritelmä 2.44** (Jakajien summa)**.** Kaikille $n\in\mathbb{Z}_+$

$$\sigma(n)=\sum_{d|n}d \quad \text{, missä } d\in\mathbb{Z}_+.$$

*Huomautus.* Lukua $n$ kutsutaan *täydelliseksi luvuksi*, jos $\sigma(n)=2n$.

Osoitetaan seuraavaksi, että edellä esitellyt funktiot ovat multiplikatiivisia. Möbiuksen funktion yhteydessä viimeisenä todistettu lause 2.42 osoittaa voimansa jo nyt. Lisäksi todistetaan lausekkeet, joilla funktioiden arvot voidaan laskea mille tahansa positiiviselle kokonaisluvulle.

**Lause 2.45.** *Jakajien lukumäärä -funktio $\tau$ on multiplikatiivinen.*

*Todistus.* Olkoon $f(n) = 1$. Nyt $f$ on täydellisesti multiplikatiivinen ja

$$\tau(n) = \sum_{d|n} f(d).$$

Tulos seuraa lauseen 2.42 nojalla. □

**Lause 2.46.** *Jakajien summa -funktio $\sigma$ on multiplikatiivinen.*

*Todistus.* Olkoon $f(n) = n$. Nyt $f$ on täydellisesti multiplikatiivinen ja

$$\sigma(n) = \sum_{d|n} f(d).$$

Tämäkin tulos seuraa nyt lauseesta 2.42. □

**Apulause 2.47.** *Olkoon $p$ alkuluku ja olkoon $a \in \mathbb{Z}_+$. Tällöin*

$$\tau(p^a) = a + 1.$$

*Todistus.* Luvun $p^a$ jakajat ovat $1, p, p^2, ..., p^{a-1}, p^a$. Jakajia on selvästi $a + 1$ kappaletta, joten $\tau(p^a) = a + 1$. □

**Apulause 2.48.** *Olkoon $p$ alkuluku ja olkoon $a \in \mathbb{Z}_+$. Tällöin*

$$\sigma(p^a) = \frac{p^{a+1} - 1}{p - 1}.$$

*Todistus.* Selvästi

$$\sigma(p^a) = \sum_{d|p^a} d = \sum_{i=0}^{a} p^i$$

ja operoidaan yhtälöä puolittain kertomalla luvulla $p$. Saadaan

$$p\sigma(p^a) = p \sum_{i=0}^{a} p^i = \sum_{i=0}^{a} p^{i+1}.$$

Nyt, kun muutetaan indeksointia siten, että $j = i + 1$, saadaan

$$\sum_{i=0}^{a} p^{i+1} = \sum_{j=1}^{a+1} p^j = \sum_{j=0}^{a} p^j + p^{a+1} - 1.$$

Viimeinen kohta perustellaan seuraavasti: koska summa alkaa $j$-indeksistä nolla, pitää indeksiä $j = 0$ vastaava summattava vähentää, sillä sellaista ei ole alkuperäisessä summassa. Samaten pitää lisätä indeksiä $j = a + 1$ vastaava termi, koska se jää pois summasta, jossa summataan vain indeksiin $j = a$ asti. Huomataan, että $\sum_{j=0}^{a} p^j = \sigma(p^a)$, joten yhtälöstä saadaan

$$\begin{aligned} p\sigma(p^a) - \sigma(p^a) &= p^{a+1} - 1 \\ \sigma(p^a)(p-1) &= p^{a+1} - 1 \\ \sigma(p^a) &= \frac{p^{a+1} - 1}{p - 1} \end{aligned}$$

ja lause on todistettu. □

Näiden apulauseiden avulla seuraavat kaksi lausetta ovat helppoja todistettavia.

**Lause 2.49.** *Olkoot* $n = \prod_{i=1}^{k} p_i^{a_i}$ *ja* $a \in \mathbb{Z}$. *Tällöin*

$$\tau(n) = \prod_{i=1}^{k} (a_i + 1).$$

*Todistus.* Koska luvun $n$ tekijät ovat keskenään jaottomia, voidaan hyödyntää funktion $\tau$ multiplikatiivisuutta. Siis

$$\tau(n) = \tau\left(\prod_{i=1}^{k} p_i^{a_i}\right) = \prod_{i=1}^{k} \tau(p_i^{a_i}) = \prod_{i=1}^{k} (a_i + 1).$$

□

**Lause 2.50.** *Olkoot* $n = \prod_{i=1}^{k} p_i^{a_i}$ *ja* $a \in \mathbb{Z}$. *Tällöin*

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$

*Todistus.* Vastaavasti kuin edellä saadaan funktion $\sigma$ multiplikatiivisuuden nojalla

$$\sigma(n) = \sigma\left(\prod_{i=1}^{k} p_i^{a_i}\right) = \prod_{i=1}^{k} \sigma(p_i^{a_i}) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$

□

# 3 Eulerin $\phi$-funktio

## 3.1 Määritelmä

**Määritelmä 3.1** (Eulerin $\phi$-funktio)**.** Kaikille $n > 0$

$$\phi(n) = |\{1 \leq a \leq n : (a, n) = 1\}|,$$

eli Eulerin $\phi$-funktio palauttaa luvun $n$ kanssa keskenään jaottomien lukujen, jotka eivät ole sitä suurempia, lukumäärän. Käytännöllisyyden vuoksi on sovittu, että $\phi(1) = 1$.

Voidaan todeta, että $\phi(n)$ on supistetun jäännössysteemin modulo $n$ alkioiden lukumäärä.

**Esimerkki 3.1.** Ohessa on lueteltu $\phi$-funktion arvoja joillakin syötteillä.

| $x$ | $\phi(x)$ | $x$ | $\phi(x)$ |
|---|---|---|---|
| 1 | 1 | 10 | 4 |
| 2 | 1 | 20 | 8 |
| 3 | 2 | 30 | 8 |
| 4 | 2 | 50 | 20 |
| 5 | 4 | 100 | 40 |

Lukuteoreettisessa mielessä monet $\phi$-funktion ominaisuuksista ovat varsin mielenkiintoisia, joten katsastetaan, millaisia ominaisuuksia funktio sisäänsä kätkee.

## 3.2 Multiplikatiivisuus

Eräs tärkeimpiä $\phi$-funktion ominaisuuksia on sen multiplikatiivisuus. Eulerin $\phi$-funktion summafunktio on erittäin elegantti ja se esitellään ensin, koska tulosta tarvitaan multiplikatiivisuuden todistuksessa.

**Lause 3.2.** *Olkoon $n \in \mathbb{Z}_+$. Tällöin*

$$\sum_{d|n} \phi(d) = n.$$

*Todistus.* Vrt. [6, s. 244]. Jaetaan luvut $1, 2, ..., n$ joukkoihin

$$n_d = \{m \in \mathbb{Z} : 1 \leq m \leq n, (m, n) = d\}$$

eli jokainen luvuista $1, 2, ...n$ on täsmälleen yhdessä joukossa $n_d$. Koska $(m, n) = d$, niin $(\frac{m}{d}, \frac{n}{d}) = 1$. Jokaisen joukon alkioiden lukumäärä on siis $|n_d| = \phi(\frac{n}{d})$ eli luvun $\frac{n}{d}$ kanssa keskenään jaottomien lukujen lukumäärä. Koska lukuja on kaikkiaan $n$ kappaletta, on kaikkien joukkojen alkioiden lukumäärien summa $n$. Siis

$$\sum_{d|n} \phi(d) = \sum_{d|n} \phi(\frac{n}{d}) = n.$$

□

Tämän jälkeen Möbiuksen funktion yhteydessä esitettyjen tulosten avulla multiplikatiivisuus on helppo todistaa ja se tehdään seuraavassa lauseessa.

**Lause 3.3.** *Eulerin $\phi$-funktio on multiplikatiivinen eli*

$$\phi(mn) = \phi(m)\phi(n), \quad kun\ (m, n) = 1.$$

*Todistus.* Vrt. [10, s. 163]. Olkoon $g(n) = n$. Funktio $g$ on tällöin täydellisesti multiplikatiivinen. Lauseen 3.2 perusteella $n = \sum_{d|n} \phi(d)$. Nyt siis

$$g(n) = \sum_{d|n} \phi(d)$$

ja tulos seuraa lauseen 2.42 nojalla. □

## 3.3 Funktion arvo

Seuraavaksi todistetaan lause, jossa $\phi$-funktio kytkeytyy alkulukuihin. Funktion $\phi$ avulla voidaan siis antaa ehto, milloin luku on alkuluku.

**Lause 3.4.** *Jos $p$ on alkuluku, niin $\phi(p) = p - 1$. Käänteisesti, jos $\phi(p) = p - 1$, niin $p$ on alkuluku.*

*Todistus.* Vrt. [6, s. 240]. Oletetaan ensin, että $p$ on alkuluku, jolloin jokainen lukua $p$ pienempi positiivinen kokonaisluku on jaoton luvun $p$ kanssa. Koska tällaisia lukuja on $p-1$, niin $\phi(p) = p-1$. Oletetaan sitten, että $\phi(p) = p-1$. Nyt jos $p$ ei ole alkuluku, niin joko $p = 1$ tai luvulla $p$ on aidot tekijät. Jos $p = 1$, niin $\phi(p) \neq p-1$, koska $\phi(1) = 1$. Jos luvulla $p$ on aidot tekijät, niin sillä on oltava jakaja $d : 1 < d < p$ ja $(p, d) > 1$. Nyt siis tiedetään, että jos jokin luvuista $2, ..., p-1$ eli $d$ ei ole luvun $p$ kanssa jaoton, niin $\phi(p) \leq p-2$. Tämä on ristiriita, joten jos $\phi(p) = p-1$, niin luvun $p$ on oltava alkuluku. □

**Lause 3.5.** *Kaikille* $n \geq 2$

$$\phi(n) \leq n - 1.$$

*Todistus.* Tulos seuraa funktion $\phi$ määritelmästä ja lauseesta 3.4. □

**Lause 3.6.** *Olkoon* $p$ *alkuluku ja* $k \in \mathbb{Z}$. *Tällöin*

$$\phi(p^k) = p^k - p^{k-1}.$$

*Todistus.* Vrt. [6, s. 241]. Kaikki lukua $p^k$ pienemmät tai yhtäsuuret luvut, joiden suurin yhteinen tekijä luvun $p^k$ kanssa on suurempi kuin 1, ovat $p, 2p, 3p, ..., p^{k-1}p$. Näitä lukuja on selvästi $p^{k-1}$. Siis luvun $p^k$ kanssa keskenään jaottomia lukuja on $p^k - p^{k-1}$ eli $\phi(p^k) = p^k - p^{k-1}$. □

Viimeisimmän lauseen avulla voidaan osoittaa muun muassa seuraava $\phi$-funktion mielenkiintoista luonnetta kuvaava tulos.

**Lause 3.7.** *Olkoon* $n \in \mathbb{Z}_+$. *Tällöin* $\phi(n)$ *on parillinen, jos* $n > 2$, *ja* $\phi(n) = 1$ *muulloin.*

*Todistus.* Olkoon $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. Koska $\phi$ on multiplikatiivinen funktio, niin

$$\phi(n) = \prod_{i=1}^{k} \phi(p_i^{a_i}) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1).$$

Nyt $\phi(n)$ on parillinen, jos jokin sen tekijöistä on parillinen. Jos mikä tahansa $p_i$ on pariton, niin $p_i - 1$ on parillinen ja edelleen $\phi(n)$ on parillinen. Jos sen

sijaan jokin $p_i$ on parillinen, niin tällöin pitää olla $p_i = 2$. Koska $n > 2$, niin joko vähintään yksi $p_i > 2$ ja pariton, jolloin tilanne palautuu edelliseen, tai $p_i^{a_i} = 2^{a_i}, a_i > 1$, jolloin $p_i^{a_i - 1}$ on siis parillinen. Jokin näistä ehdoista täyttyy aina, joten $\phi(n)$ on parillinen, kun $n > 2$.

Väitteen loppuosa eli tapaukset $n = 1$ ja $n = 2$ voidaan todistaa laskemalla funktion arvot näissä kohdissa

$$\phi(1) = 1 = \phi(2).$$

□

**Seuraus 3.8.** *Jos $n \in \mathbb{Z}_+$ on pariton, niin*

$$\phi(n) = \phi(2n)$$

*Todistus.* Koska $n$ on pariton, niin $(2, n) = 1$, joten

$$\phi(2n) = \phi(2)\phi(n) = 1 \cdot \phi(n) = \phi(n).$$

□

Todistetaan lauseen 3.6 avulla kaava, jolla $\phi$-funktion arvon voi laskea mille tahansa kokonaisluvulle.

**Lause 3.9.** *Olkoon $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, missä $p_i \neq p_j, \forall i, j, 1 \leq i, j \leq k$. Tällöin*

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

*Todistus.* Vrt. [6, s. 242]. Koska $\phi$ on multiplikatiivinen, niin

$$\phi(n) = \phi(p_1^{a_1})\phi(p_2^{a_2}) \cdots \phi(p_k^{a_k}).$$

Lauseen 3.6 perusteella jokainen $\phi(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i - 1} = p_i^{a_i}\left(1 - \frac{1}{p_i}\right)$, joten

$$\begin{aligned}
\phi(n) =& p_1^{a_1}\left(1 - \frac{1}{p_1}\right) p_2^{a_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{a_k}\left(1 - \frac{1}{p_k}\right) \\
=& p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\
=& n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)
\end{aligned}$$

□

Esitellään seuraavaksi tulos, jolla voi varsin mekaanisesti laskea $\phi$-funktion arvon. Ks. [9, s. 84].

**Lause 3.10.** *Olkoon* $n = \prod_{i=1}^{k} p_i^{a_i}$. *Jos*

$$e_j(p_i) = \begin{cases} 1, & jos\ p_i \mid j \\ 0, & muulloin, \end{cases}$$

*niin*

$$\phi(n) = \sum_{j=1}^{n} \prod_{i=1}^{k} (1 - e_j(p_i)).$$

*Todistus.* Tulontekijät ovat nollasta poikkeavia vain, jos $e_j(p_i) = 0$. Tulo jollakin indeksillä $j_0$ puolestaan poikkeaa nollasta vain, jos $e_{j_0}(p_i) = 0$, kaikilla $1 \leq i \leq k$. Tämä toteutuu, kun $(j_0, n) = 1$, sillä jos $(j_0, n) > 1$, niin $p_i \mid j_0$, jollakin $i$, ja tällöin $1 - e_{j_0}(p_i) = 0$ ja edelleen $\prod_{i=1}^{k}(1 - e_{j_0}(p_i)) = 0$. Nyt huomataan, että

$$\left\lfloor \frac{1}{(j,n)} \right\rfloor = \begin{cases} 1, & \text{jos } (j,n) = 1 \\ 0, & \text{muulloin,} \end{cases}$$

joten $\prod_{i=1}^{k}(1 - e_j(p_i)) = \lfloor \frac{1}{(j,n)} \rfloor$ ja tulos seuraa tästä. □

Osoitetaan vielä kaksi tulosta Eulerin $\phi$-funktion ja Möbiuksen funktion yhteydestä.

**Lause 3.11.** *Olkoon* $n \in \mathbb{Z}_+$. *Tällöin*

$$\phi(n) = n \sum_{d \mid n} \frac{\mu(d)}{d}.$$

*Todistus.* Todistetaan tulos käyttäen hyväksi Möbiuksen käänteiskaavaa. Nyt siis

$$F(n) = \sum_{d \mid n} f(d) = \sum_{d \mid n} \phi(d) = n \quad \text{ja}$$

$$f(n) = \phi(n) = \sum_{d \mid n} \mu(d) F(\frac{n}{d}) = \sum_{d \mid n} \mu(d) \frac{n}{d} = n \sum_{d \mid n} \frac{\mu(d)}{d},$$

mikä todistaa lauseen. □

**Lause 3.12.** *Olkoon $n \in \mathbb{Z}_+$. Tällöin*

$$\frac{n}{\phi(n)} = \sum_{d|n} \frac{\mu^2(d)}{\phi(d)}.$$

*Todistus.* Vrt. [1, s. 8]. Jos $n = 1$, niin väite pätee. Merkitään sitten $n = p_1^{a_1} \cdots p_k^{a_k}$, jolloin

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{k} \frac{p_i - 1}{p_i}.$$

Yhtälön vasen puoli saa muodon

$$\frac{n}{\phi(n)} = \frac{n}{n \prod_{i=1}^{k} \frac{p_i - 1}{p_i}} = \frac{p_1 \cdots p_k}{(p_1 - 1) \cdots (p_k - 1)}.$$

Käsitellään sitten yhtälön oikeaa puolta. Muistetaan, että $\mu(n) = 1$, jos $n = 1$, $\mu(n) = (-1)^k$, jos $n = p_1 \cdots p_k$ ja $\mu(n) = 0$ muulloin. Täten siis

$$\frac{\mu^2(e)}{\phi(e)} = \begin{cases} \frac{1}{\phi(e)}, & \text{jos } e \text{ on neliövapaa luvun } n \text{ jakaja eli muotoa } \prod_{i=1}^{k} p_i, \\ 0, & \text{muulloin,} \end{cases}$$

joten tällaisten termien summa on sama kuin nollasta poikkeavien termien summa. Saadaan

$$\begin{aligned} &\sum_{d|n} \frac{\mu^2(d)}{\phi(d)} = \sum_{e|n} \frac{1}{\phi(e)} \\ &= \frac{1}{1} + \frac{1}{\phi(p_1)} + \frac{1}{\phi(p_2)} + ... \frac{1}{\phi(p_k)} + \frac{1}{\phi(p_1 p_2)} + ... + \frac{1}{\phi(p_1 p_2 \cdots p_k)} \\ &= 1 + \frac{1}{p_1 - 1} + \frac{1}{p_2 - 1} ... \frac{1}{p_k - 1} + ... + \frac{1}{(p_1 - 1)(p_2 - 1) \cdots (p_k - 1)} \\ &= \frac{(p_1 - 1)(p_2 - 1) \cdots (p_k - 1) + (p_2 - 1) \cdots (p_k - 1) + ... + (p_k - 1) + 1}{(p_1 - 1)(p_2 - 1) \cdots (p_k - 1)}. \end{aligned}$$

Tässä vaiheessa huomataan, että yhtälön molemmilla puolilla on sama nimittäjä. Siirrytään tarkastelemaan osoittajia. Summausjärjestystä muuttamalla yhtälön oikealle puolelle saadaan

$$\begin{aligned} &1 + (p_1 - 1) + (p_2 - 1) + ... + (p_k - 1) + ... + (p_1 - 1)(p_2 - 1) \cdots (p_k - 1) \\ =&\phi(1) + \phi(p_1) + \phi(p_2) + ... + \phi(p_k) + \phi(p_1 p_2) + ... + \phi(p_1 p_2 \cdots p_k) \\ =& \sum_{e|p_1 p_2 \cdots p_k} \phi(e) = p_1 p_2 \cdots p_k. \end{aligned}$$

Viimeinen yhtäsuuruus pätee lauseen 3.2 nojalla. Koska myös osoittajat yhtälön molemmin puolin ovat samat, on lause todistettu. □

Koska $\phi$ ei ole täydellisesti multiplikatiivinen, sen arvon laskeminen kahden luvun tulolle ei ole aivan suoraviivaista, jos näillä luvuilla on yhteisiä tekijöitä. Muistamme, että $\phi(mn) = \phi(m)\phi(n)$ vain silloin, jos $m$ ja $n$ ovat keskenään jaottomia. Todistetaan seuraavaksi lause, jolla selviämme tilanteesta, jossa luvut eivät ole keskenään jaottomia, [9, s. 84].

**Lause 3.13.** *Olkoot $a, m, n \in \mathbb{Z}_+$ ja $(m, n) = a$. Tällöin*

$$\phi(mn) = \frac{a}{\phi(a)}\phi(m)\phi(n).$$

*Todistus.* Lasketaan auki $\phi(mn)$. Jätetään indeksit selvyyden vuoksi pois eli saadaan

$$\phi(mn) = mn \prod_{p|mn} \left(1 - \frac{1}{p}\right).$$

Nyt

$$\prod_{p|mn} \left(1 - \frac{1}{p}\right) = \frac{\prod_{p|m} \left(1 - \frac{1}{p}\right) \prod_{p|n} \left(1 - \frac{1}{p}\right)}{\prod_{p|m,p|n} \left(1 - \frac{1}{p}\right)}.$$

Koska ne luvut $p$, jotka jakavat sekä luvun $m$ että luvun $n$, ovat ne luvut $p$, jotka jakavat luvun $a$, saadaan

$$\prod_{p|m,p|n} \left(1 - \frac{1}{p}\right) = \prod_{p|a} \left(1 - \frac{1}{p}\right).$$

Palataan alkuperäiseen lausekkeeseen ja kerrotaan mukaan ykkönen. Saadaan

$$\begin{aligned}
\phi(mn) &= mn \prod_{p|mn} \left(1 - \frac{1}{p}\right) \\
&= mn \frac{\prod_{p|m} \left(1 - \frac{1}{p}\right) \prod_{p|n} \left(1 - \frac{1}{p}\right)}{\prod_{p|a} \left(1 - \frac{1}{p}\right)} \cdot \frac{a}{a} \\
&= \frac{a}{a \prod_{p|a} \left(1 - \frac{1}{p}\right)} m \prod_{p|m} \left(1 - \frac{1}{p}\right) n \prod_{p|n} \left(1 - \frac{1}{p}\right) \\
&= \frac{a}{\phi(a)} \phi(m)\phi(n)
\end{aligned}$$

ja lause on todistettu. □

## 3.4 Eulerin $\phi$ ja kongruenssi

**Lause 3.14.** *Jos* $\{a_1, a_2, ..., a_{\phi(n)}\}$ *on supistettu jäännössysteemi modulo* $n$ *ja* $(c, n) = 1$*, niin* $\{ca_1, ca_2, ..., ca_{\phi(n)}\}$ *on myös supistettu jäännössysteemi modulo* $n$*.*

*Todistus.* Olkoon $\{a_1, a_2, ..., a_{\phi(n)}\}$ supistettu jäännössysteemi modulo $n$ ja $(c, n) = 1$. Nyt koska $(c, n) = 1$ ja $(a_i, n) = 1$, niin $(ca_i, n) = 1$, kun $i = 1, 2, ..., \phi(n)$. Sovelletaan seuraavaksi kontrapositiota. Jos $ca_i \equiv ca_j \pmod{n}$ joillakin $1 \leq i < j \leq \phi(n)$, niin seurauksen 2.29 perusteella $a_i \equiv a_j \pmod{n}$.Täten siis $\{ca_1, ca_2, ..., ca_{\phi(n)}\}$ on supistettu jäännössysteemi modulo $n$. □

Jatketaan kohti merkittävää tulosta, joka on Eulerin-Fermat'n lause (vrt. [10, s. 165].

**Lause 3.15** (Eulerin-Fermat'n lause)**.** *Olkoon* $(a, n) = 1$*. Tällöin*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

*Todistus.* Olkoon $\{a_1, a_2, ..., a_{\phi(n)}\}$ supistettu jäännössysteemi modulo $n$. Koska $(a, n) = 1$, niin lauseen 3.14 nojalla myös $\{a \cdot a_1, a \cdot a_2, ..., a \cdot a_{\phi(n)}\}$ on supistettu jäännössysteemi. Tällöin jokaiselle $i, 1 \leq i \leq \phi(n)$ on olemassa sellainen kokonaisluku $j, 1 \leq j \leq \phi(n)$, että $a \cdot a_i \equiv a_j \pmod{n}$. Koska kongruenssi säilyy kertolaskussa lauseen 2.27 perusteella, niin voidaan kertoa kunkin jäännössysteemin alkiot keskenään. Tästä seuraa, että

$$\prod_{i=1}^{\phi(n)} (a \cdot a_i) \equiv \prod_{j=1}^{\phi(n)} a_j \pmod{n}$$

$$\Leftrightarrow \quad a^{\phi(n)} \prod_{i=1}^{\phi(n)} a_i \equiv \prod_{j=1}^{\phi(n)} a_j \pmod{n}.$$

Koska $(\prod_{i=1}^{\phi(n)} a_i, n) = 1$, niin tulos

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

seuraa seurauksen 2.29 perusteella. □

Koska $\phi(n) > 0$ kaikilla $n \in \mathbb{Z}_+$, niin Eulerin-Fermat'n lauseen perusteella on olemassa vähintään yksi sellainen kokonaisluku $x$, että $a^x \equiv 1 \pmod{n}$. Annetaan tällaiselle luvulle tarkka määritelmä. [3].

**Määritelmä 3.16** (Kokonaisluvun kertaluku modulo $n$)**.** Olkoot $a \in \mathbb{Z}$, $n \in \mathbb{Z}_+$ sekä $(a, n) = 1$. Tällöin luvun $a$ *kertaluku modulo* $n$ on pienin sellainen positiivinen kokonaisluku $x$, että $a^x \equiv 1 \pmod{n}$. Merkitään $x = ord_n a$.

Todistetaan eräs kokonaisluvun kertalukuun liittyvä tulos, jonka seurauksen voimme kytkeä Eulerin $\phi$-funktion ominaisuuksiin [3].

**Lause 3.17.** *Olkoot $a \in \mathbb{Z}$, $n \in \mathbb{Z}_+$ sekä $(a, n) = 1$. Tällöin*

$$a^x \equiv 1 \pmod{n} \Leftrightarrow ord_n a \mid x.$$

*Todistus.* Oletetaan ensin, että $ord_n a \mid x$ eli on olemassa sellainen kokonaisluku $k$, että $x = (ord_n a)k$. Nyt

$$a^x = (a^{ord_n a})^k \equiv 1^k = 1 \pmod{n}.$$

Ensimmäinen vaihe on täten todistettu, joten oletetaan, että $a^x \equiv 1 \pmod{n}$. Jakoalgoritmin mukaan

$$x = (ord_n a)q + r \quad , \quad \text{missä } 0 \leq r < ord_n a.$$

Nyt siis

$$a^x = a^{(ord_n a)q + r} = a^{(ord_n a)q} a^r \equiv a^r \pmod{n}.$$

Koska $a^x \equiv 1 \pmod{n}$, niin $a^r \equiv 1 \pmod{n}$. Täten epäyhtälön $0 \leq r < ord_n a$ ja kokonaisluvun kertaluvun määritelmän perusteella $r = 0$. Näin ollen $x = (ord_n a)q + r = (ord_n a)q$ eli $ord_n a \mid x$. □

**Seuraus 3.18.** *Jos $a \in \mathbb{Z}$, $n \in \mathbb{Z}_+$ sekä $(a, n) = 1$, niin $ord_n a \mid \phi(n)$.*

**Lause 3.19.** *Olkoon $p$ alkuluku, $a \in \mathbb{Z}$ ja $p \nmid a$. Tällöin*

$$a^{p-1} \equiv 1 \pmod{p}.$$

*Todistus.* Koska $(a, p) = 1$, niin lauseen 3.15 nojalla

$$a^{p-1} = a^{\phi(p)} \equiv 1 \pmod{p}.$$

□

**Lause 3.20.** *Olkoon $n \in \mathbb{Z}$ ja $n > 2$. Tällöin*

$$\phi(n) \equiv 0 \pmod{2}.$$

*Todistus.* Lauseessa sanotaan kongruenssin keinoin, että $\phi(n)$ on parillinen, kun $n > 2$. Todistus on siis annettu lauseessa 3.7. □

Seuraavan tuloksen on lähteiden mukaan ensimmäisenä esittänyt Umberto Scarpis. Todistetaan italialaisen löytämä ominaisuus.

**Lause 3.21.** *Olkoot $a \in \mathbb{Z}$, $n \in \mathbb{Z}_+$. Tällöin*

$$\phi(a^n - 1) \equiv 0 \pmod{n} \quad eli \quad n \mid \phi(a^n - 1).$$

*Todistus.* Vrt. [8, s. 202]. Merkitään

$$A = a^n - 1,$$

jolloin siis $a^n = A + 1$. Tällöin selvästi $a^n \equiv 1 \pmod{A}$ ja $(a, A) = 1$. Seurauksen 3.18 perusteella $n = ord_A a \mid \phi(A) = \phi(a^n - 1)$. □

Eulerin $\phi$-funktiolla on mielenkiintoisia yhteyksiä lukuihin, joiden lukumäärän se laskee. Katsotaan muutama lause, joissa supistetun jäännössysteemin termien avulla saadaan funktiota $\phi$ koskevia tuloksia. [5].

**Lause 3.22.** *Olkoot $a_1, ..., a_{\phi(n)}, n \in \mathbb{Z}_+$, $a_i \leq n$ ja $(a_i, n) = 1$ kaikilla $1 \leq i \leq \phi(n)$. Tällöin, jos $n \geq 2$, niin*

$$a_1 + a_2 + ... + a_{\phi(n)} = \frac{n\phi(n)}{2}.$$

*Todistus.* Koska $(a_i, n) = 1$, niin lauseen 2.17 perusteella myös $(n - a_i, n) = 1$. Tämän seurauksena voidaan kirjoittaa

$$\{a_1, a_2, ..., a_{\phi(n)}\} = \{n - a_1, n - a_2, ..., n - a_{\phi(n)}\}.$$

Koska joukkojen alkiot ovat samat (oikeanpuoleisessa alkioiden järjestys on käänteinen), ovat myös joukkojen alkioiden summat samat eli

$$\begin{aligned} a_1 + a_2 + ... + a_{\phi(n)} &= (n - a_1) + (n - a_2) + ... + (n - a_{\phi(n)}) \\ &= n\phi(n) - (a_1 + a_2 + ... + a_{\phi(n)}), \end{aligned}$$

mistä saadaan

$$a_1 + a_2 + ... + a_{\phi(n)} = \frac{n\phi(n)}{2}.$$

□

**Lause 3.23.** *Olkoon $n \geq 3$ ja olkoot $a_1, ..., a_{\phi(n)} \in \mathbb{Z}_+, a_i \leq n$ ja $(a_i, n) = 1$ kaikilla $1 \leq i \leq \phi(n)$. Tällöin*

$$a_1 + a_2 + ... + a_{\phi(n)} \equiv 0 \pmod{n}.$$

*Todistus.* Lauseen 3.22 perusteella $a_1 + a_2 + ... + a_{\phi(n)} = \frac{n\phi(n)}{2}$. Lisäksi, kun $n \geq 3$, lause 3.7 kertoo, että $\phi(n)$ on parillinen. Merkitään $\phi(n) = 2k$, missä $k \in \mathbb{Z}_+$. Nyt

$$a_1 + a_2 + ... + a_{\phi(n)} = \frac{n\phi(n)}{2} = \frac{n2k}{2} = nk \equiv 0 \pmod{n}.$$

□

**Lause 3.24.** *Olkoot $a_1, ..., a_{\phi(n)}, n \in \mathbb{Z}_+$, $a_i \leq n$ ja $(a_i, n) = 1$ kaikilla $1 \leq i \leq \phi(n)$. Tällöin kaikilla $i \in \{1, 2, ..., \phi(n)\}$*

$$a_i = n - a_{\phi(n)-i+1}.$$

*Todistus.* Nyt $a_1 < a_2 < ... < a_{\phi(n)-1} < a_{\phi(n)}$. Tällöin selvästi $n - a_{\phi(n)} < n - a_{\phi(n)-1} < ... < n - a_2 < n - a_1$. Vastaavat termit ovat yhtäsuuria, joten saadaan

$$a_1 = n - a_{\phi(n)}, \quad a_2 = n - a_{\phi(n)-1}, \ ... \ , a_{\phi(n)-1} = n - a_2, \quad a_{\phi(n)} = n - a_1,$$

mistä tulos seuraa eli $a_i = n - a_{\phi(n)-i+1}$. □

**Lause 3.25.** *Olkoot* $a_1, ..., a_{\phi(n)}, n \in \mathbb{Z}_+, a_i \leq n$ *ja* $(a_i, n) = 1$ *kaikilla* $1 \leq i \leq \phi(n)$. *Kaikille* $n \geq 3$

$$a_1^2 + a_2^2 + ... + a_{\phi(n)}^2 + ... + 2(a_1 a_{\phi(n)} + a_2 a_{\phi(n)-1} + ... + a_{\frac{\phi(n)}{2}} a_{\frac{\phi(n)}{2}+1}) = \frac{n^2\phi(n)}{2}.$$

*Todistus.* Aloitetaan todistus toteamalla kaksi seikkaa. Ensinnä $\phi(n)$ on parillinen, kun $n \geq 3$, eli $\frac{\phi(n)}{2} \in \mathbb{Z}$. Toisekseen lauseen 3.24 perusteella $a_i = n - a_{\phi(n)-i+1}$, mistä seuraa, että $a_{\phi(n)-i+1} = n - a_i$. Tällöin

$$\sum_{i=1}^{\phi(n)} a_i a_{\phi(n)-i+1} = a_1 a_{\phi(n)} + a_2 a_{\phi(n)-1} + ... + a_{\phi(n)-1} a_{\phi(n)-(\phi(n)-1)+1} + a_{\phi(n)} a_1.$$

Huomataan, että kukin termi on kahteen kertaan, joten saadaan

$$\sum_{i=1}^{\phi(n)} a_i a_{\phi(n)-i+1} = 2(a_1 a_{\phi(n)} + a_2 a_{\phi(n)-1} + ... + a_{\frac{\phi(n)}{2}} a_{\frac{\phi(n)}{2}+1}) = \sum_{i=1}^{\phi(n)} a_i(n - a_i).$$

Sijoitetaan summalauseke väitteen kaavaan, jolloin saadaan

$$\sum_{i=1}^{\phi(n)} a_i^2 + \sum_{i=1}^{\phi(n)} a_i(n - a_i) = \sum_{i=1}^{\phi(n)} a_i^2 + n\sum_{i=1}^{\phi(n)} a_i - \sum_{i=1}^{\phi(n)} a_i^2 = n\sum_{i=1}^{\phi(n)} a_i.$$

Lause 3.22 osaa kertoa, että

$$\sum_{i=1}^{\phi(n)} a_i = \frac{n\phi(n)}{2},$$

joten

$$n\frac{n\phi(n)}{2} = \frac{n^2\phi(n)}{2}$$

ja tulos seuraa tästä. □

Seuraavan tuloksen esitti ensimmäisenä D. H. Lehmer, joka esitti kysymyksen, onko olemassa yhdistettyä lukua $n$, joka toteuttaisi ehdon $\phi(n) \mid n-1$ vai onko tällainen luku aina alkuluku. Tällaista yhdistettyä lukua ei ole vielä löydetty ja kysymys on yhä avoin. Todistetaan seuraavaksi Lehmerin tulos, joka koskee tämän ehdon täyttäviä lukuja. [8, s. 212].

**Lause 3.26.** *Olkoon $n \in \mathbb{Z}_+$. Jos $\phi(n) \mid n-1$, niin $n$ on alkuluku tai $n$ on neliövapaa ja pariton yhdistetty luku.*

*Todistus.* Jos $n$ on alkuluku, niin $1 \cdot \phi(n) = \phi(n) = n-1$, joten alkuluku toteuttaa aina ehdon $\phi(n) \mid n-1$.

Oletetaan sitten, että $n$ ei ole alkuluku, joten olkoon $n = \prod_{i=1}^{k} p_i^{a_i}$. Tällöin $p_i^{a_i} \mid n$ ja myös $p_i^{a_i-1} \mid n$ kaikilla $1 \leq i \leq k$. Nyt

$$\phi(n) = \prod_{i=1}^{k} p_i^{a_i-1}(p_i - 1)$$

eli $p_i^{a_i-1} \mid \phi(n)$ ja edelleen oletuksen perusteella $\phi(n) \mid n-1$, joten $p_i^{a_i-1} \mid n-1$. Koska $p_i^{a_i-1} \mid n$ ja $p_i^{a_i-1} \mid n-1$, on oltava $a_i = 1$. Luku $n$ on siis neliövapaa.

Oletetaan sitten, että $n$ on parillinen. Merkitään $n = 2q$, missä $q = \prod p > 2$ on jokin pariton luku (indeksointi on selkeyden vuoksi jätetty pois). Nyt

$$\phi(n) = \phi(2)\phi(q) = \prod (p-1) \mid n-1$$

eli $\prod(p-1)$ on parittoman luvun $n-1$ tekijä. Lauseen 3.7 perusteella $\phi(q)$ on kuitenkin parillinen, joten seuraa ristiriita. Tästä syystä luvun $n$ on oltava pariton ja lause on todistettu. □

**Lause 3.27.** *Olkoot $m, n \in \mathbb{Z}_+$ ja $m \mid n$. Tällöin $\phi(m) \mid \phi(n)$.*

*Todistus.* Olkoon $m = \prod_{i=1}^{k} p_i^{a_i}$ sekä olkoot $q = \prod_{p_i \mid m} p_i^{b_i}$, missä $b_i \geq a_i$, ja $r \in \mathbb{Z}_+, (m, r) = 1$ sellaisia, että $n = qr$. Nyt koska $q$ kattaa vain ne alkuluvut, jotka ovat luvun $m$ tekijöitä, ja $(m, r) = 1$, niin $(q, r) = 1$. Tällöin

$$\frac{\phi(n)}{\phi(m)} = \frac{\phi(qr)}{\phi(m)} = \frac{\phi(q)\phi(r)}{\phi(m)} = \frac{\prod_{i=1}^{k} p_i^{b_i-1}(p_i-1)}{\prod_{i=1}^{k} p_i^{a_i-1}(p_i-1)}\phi(r) = \prod_{i=1}^{k} p_i^{b_i-a_i}\phi(r) \in \mathbb{Z}$$

tarkoittaen sitä, että $\phi(n)$ voidaan esittää tulona, jossa toinen tekijä on $\phi(m)$ ja toinen jokin kokonaisluku, eli $\phi(m) \mid \phi(n)$. □

## 3.5 Eulerin $\phi$ yhtälöissä ja identiteettejä

Olemme osoittaneet tuloksia, joilla $\phi$-funktion arvon pystyy laskemaan. Osoitimme myös joitakin funktion ominaisuuksia muun muassa kongruenssiin liittyen. Entä jos kyseessä ei olekaan kaikilla kokonaisluvuilla tosi yhtälö? Toteutuuko yhtälö millään kokonaisluvuilla? Tarkastellaan siis seuraavaksi, kuten Sándor tekee, millä arvoilla tietyt yhtälöt, joissa $\phi$ esiintyy, ovat tosia [7, ss. 108–112]. Ks. myös [8, s. 230]. Merkitään jatkossa $n \in \mathbb{P}$ silloin, jos $n$ on alkuluku. Tässä kappaleessa todistetaan myös muita vastaavia tuloksia sekä funktion $\phi$ ja muita aritmeettisia funktioita sisältäviä identiteettejä.

**Lause 3.28.** *Yhtälön*

$$\tau(n) + \phi(n) = n + 1$$

*ainoat ratkaisut ovat* $n = 1$, $n = 4$ *ja* $n \in \mathbb{P}$. *Muulloin* $\tau(n) + \phi(n) < n + 1$.

*Todistus.* Todetaan ensin, että $n = 1$, $n = 4$ ja $n \in \mathbb{P}$ ovat ratkaisuja.

$$\begin{aligned}
&\tau(1) + \phi(1) = 1 + 1, \\
&\tau(4) + \phi(4) = 3 + 2 = 4 + 1, \\
&\tau(p) + \phi(p) = (1 + 1) + (p - 1) = p + 1.
\end{aligned}$$

Oletetaan sitten, että $n > 4$ ja että $n$ on yhdistetty luku. Merkitään $d \in D_\tau(n)$, jos $d \mid n$. Eli luvut $d$ ovat luvun $n$ jakajia, jotka siis $\tau$ määritelmänsä mukaisesti laskee, joten $\tau(n) = |D_\tau(n)|$. Merkitään vastaavasti $e \in D_\phi(n)$, jos $(e, n) = 1$. Jäljelle jääneistä luvuista $\phi$ siis laskee luvut $e$ ja ykkösen ja $\phi(n) = |D_\phi(n)|$. Loppuja lukuja ei laske kumpikaan. Merkitköön $D_0(n)$ näiden lukujen joukkoa. Koska yhteensä laskettavia lukuja on korkeintaan $n$ kappaletta sekä $\tau$ ja $\phi$ molemmat laskevat ykkösen, niin

$$|D_\tau(n)| + |D_\phi(n)| + |D_0(n)| \leq n + 1.$$

Osoitetaan, että $|D_0(n)| \geq 1$. Jos $n = 2^k$, missä $k \geq 3$, niin $6 \in D_0(n)$. Jos taas $n = ap$, missä $p \in \mathbb{P}, p \neq 2$ ja $a > 1$, niin $a(p - 1) \in D_0(n)$. Siis $|D_0(n)| \geq 1$. Koska siis $|D_0(n)| \geq 1$, niin $\tau(n) + \phi(n) < n + 1$. □

**Lause 3.29.** *Yhtälön*

$$\phi(n) = \tau(n)$$

*ainoat ratkaisut ovat* $n \in \{1, 3, 8, 10, 18, 24, 30\}$. *Lisäksi, jos* $n > 30$, *niin* $\phi(n) > \tau(n)$.

*Todistus.* Selvästi $n = 1$ on ratkaisu. Oletetaan sitten, että $n = \prod_{i=1}^{k} p_i^{a_i}$, missä $a_i > 0$, on ratkaisu. Tällöin funktioiden multiplikatiivisuudesta seuraa, että

$$\frac{\phi(n)}{\tau(n)} = \frac{\prod_{i=1}^{k} \phi(p_i^{a_i})}{\prod_{i=1}^{k} \tau(p_i^{a_i})} = 1.$$

Riittää tutkia yksittäistä alkulukupotenssia (jätetään indeksit selkeyden vuoksi pois) eli

$$\frac{\phi(p^a)}{\tau(p^a)} = \frac{p^{a-1}(p-1)}{a+1}.$$

Todistetaan seuraavaksi induktiolla, että kun $p = 3$, niin $p^{a-1}(p-1) \geq a+1$. Kun $a = 1$, niin $3^{1-1}(3-1) = 2 = 1+1$. Väite on siis tosi, kun $a = 1$ ja lisäksi $n = 3$ on ratkaisu. Tehdään induktio-oletus, että väite pätee, kun $a = m$ eli $3^{m-1} \cdot 2 \geq m + 1$. Osoitetaan sitten, että väite pätee, kun $a = m + 1$. Nyt $3^{m+1-1} \cdot 2 = 3 \cdot 3^{m-1} \cdot 2$. Induktio-oletuksen nojalla saadaan $3 \cdot 3^{m-1} \cdot 2 \geq 3 \cdot (m+1) \geq m + 1 + 1 = m + 2$. Induktioperiaatteen nojalla väitteemme on tosi. Selvästi $p^{a-1}(p-1) \geq a+1$ pätee, kun $p > 3, a \geq 1$. Siis jos $n \geq 3$ ja $n$ on pariton, niin $\phi(n) \geq \tau(n)$.

Tutkitaan sitten, mitä tapahtuu, kun $n$ on parillinen. Olkoon siis $n = 2^a q$, missä $q$ on jokin pariton luku. Nyt

$$\phi(2^a q) = \phi(2^a)\phi(q) = 2^{a-1} \cdot (2-1)\phi(q) \geq 2^{a-1}\tau(q),$$

missä käytettiin $\phi$-funktion multiplikatiivisuutta ja äskeistä välitulosta. Tässä epäyhtälössä yhtäsuuruus voidaan saada vain, jos $q = 1$ tai $q = 3$ ja jos $2^{a-1} = \tau(2^a) = a + 1$. Nyt jos $a = 3$, niin $2^2 = 4 = 3 + 1$ eli $n = 2^a q$ generoi ratkaisun, jos $a = 3$ ja $q \in \{1, 3\}$. Täten siis $\phi(n) = \tau(n)$, jos $n$ on parillinen ja $a = 3$ eli $2^3 = 8 \mid n$. Ratkaisuja ovat siis $n = 1 \cdot 8$ ja $n = 3 \cdot 8$:

$$\phi(8) = \phi(2^3) = 2^2 \cdot 1 = 4 \qquad \tau(8) = \tau(2^3) = 3 + 1 = 4$$
$$\phi(24) = \phi(2^3)\phi(3) = 2^2 \cdot 1 \cdot 2 = 8 \qquad \tau(24) = \tau(2^3)\tau(3) = (3+1) \cdot 2 = 8.$$

Vastaavasti kuin edellä, voidaan induktiolla osoittaa, että $2^{a-1} > a+1$, kun $a > 3$. Analogia on täsmälleen vastaava, joten todistuksen auki kirjoittaminen sivuutetaan.

Vielä on selvitettävä tapaukset, joissa $a = 1$ tai $a = 2$. Kun $a = 1$, niin

$$\phi(2q) = \phi(2)\phi(q) = \phi(q)$$
$$\tau(2q) = \tau(2)\tau(q) = 2\tau(q).$$

Siis

$$\frac{\phi(n)}{\tau(n)} = \frac{\phi(2q)}{\tau(2q)} = \frac{\phi(q)}{2\tau(q)} = 1$$

eli

$$\frac{\phi(q)}{\tau(q)} = 2.$$

Olkoon nyt $q = \prod_{p\geq 3} p^b$ (indeksit on selvyyden vuoksi jätetty pois), jolloin saadaan

$$\frac{\phi(q)}{\tau(q)} = \prod_{p\geq 3} \frac{p^{b-1}(p-1)}{b+1} = 2.$$

Tarkastellaan taas yksittäistä alkulukupotenssia. Nyt jos $p = 3$ ja $b = 1$, niin

$$\frac{3^0(3-1)}{1+1} = \frac{2}{2} = 1,$$

joka ei yksinään tuota ratkaisua. Tarkastellaan sitten tapausta $b = 2$. Saadaan

$$\frac{3^1 \cdot 2}{2+1} = \frac{6}{3} = 2,$$

jolloin on löydetty yksi ratkaisu lisää. Siis $a = 1, q = 3, b = 2$ eli $n = 2 \cdot 3^2 = 18$. Sándor jättää jostakin syystä tämän ratkaisun pois ensimmäisessä edellä mainituista lähteistä. Induktiolla voidaan aiemmin esitetyllä tavalla todistaa, että jos $b \geq 3$, niin $3^{b-1} \cdot 2 > 2(b+1)$. Tutkitaan seuraavaksi tilannetta, jossa $p = 5$. Jos $b = 1$, niin

$$\frac{5^0(5-1)}{1+1} = \frac{4}{2} = 2.$$

Saadaan siis ratkaisu, jos $q = 5$. Täten, jos $b = 1$, saadaan toinenkin ratkaisu, kun $q = \prod_{3\leq p\leq 5} p^1$, nimittäin

$$\prod_{3\leq p\leq 5} \frac{p^{1-1}(p-1)}{1+1} = \frac{3-1}{1+1} \cdot \frac{5-1}{1+1} = \frac{2}{2} \cdot \frac{4}{2} = 2.$$

Löydetyt ratkaisut ovat siis $n = 2 \cdot 5 = 10$ ja $n = 2 \cdot 3 \cdot 5 = 30$. Jälleen induktiolla voidaan todistaa edellisiä vastaavasti, että jos $p = 5$ ja $b \geq 2$, niin $5^{b-1} \cdot 4 > 2(b+1)$. Edelleen vastaavaan tapaan voidaan todistaa, että jos $p \geq 7$ ja $b \geq 1$, niin $p^{b-1}(p-1) > 2(b+1)$.

Viimeisenä tutkitaan tilanne, kun $a = 2$. Tällöin

$$\phi(2^2 q) = \phi(2^2)\phi(q) = 2\phi(q)$$
$$\tau(2^2 q) = \tau(2^2)\tau(q) = 3\tau(q).$$

Vastaavasti kuin edellä saadaan tarkasteltavaksi yhtälö

$$\frac{\phi(q)}{\tau(q)} = \frac{p^{b-1}(p-1)}{b+1} = \frac{3}{2}.$$

Tähän mennessä on todettu, että

$$\frac{3^b \cdot 2}{b+1} > \frac{3}{2} \quad , \quad \text{jos } b > 1 \text{ sekä}$$
$$\frac{p^b(p-1)}{b+1} \geq 2 \quad , \quad \text{jos } p \geq 5, b \geq 1.$$

Jos $n$ on parillinen ja $a = 2$, niin yhtään ratkaisua ei ole.

Kaiken edellä esitetyn päättelyn perusteella voidaan siis todeta, että jos $n \in \{1, 3, 8, 10, 18, 24, 30\}$, niin

$$\phi(n) = \tau(n),$$

ja jos $n > 30$, niin

$$\phi(n) > \tau(n).$$

□

**Lause 3.30.**

$$\phi(n)\tau(n) = \phi(n) + n - 1,$$

*jos* $n \in \mathbb{P}$ *tai* $n = 1$, *ja muulloin*

$$\phi(n)\tau(n) \geq \phi(n) + n - 1.$$

*Todistus.* Oletetaan ensin, että luku $n$ on yhdistetty luku. Lauseen 3.2 perusteella $\sum_{d|n} \phi(d) = n$. Lisäksi jos $d \mid n$, niin lauseen 3.27 perusteella $\phi(d) \mid \phi(n)$ ja edelleen lauseen 2.14 nojalla $\phi(d) \leq \phi(n)$. Nyt

$$\begin{aligned} n =& \sum_{d|n} \phi(d) = 1 + \sum_{d|n, d>1} \phi(d) \leq 1 + \phi(n) \sum_{d|n, d>1} 1 \\ =& 1 + \phi(n)\left(\tau(n) - 1\right) = 1 + \phi(n)\tau(n) - \phi(n), \end{aligned}$$

mistä seuraa, että

$$\phi(n)\tau(n) \geq \phi(n) + n - 1$$

eli jos $n$ on yhdistetty luku, väitös pätee. Väite pätee selvästi, jos $n = 1$, joten oletetaan, että $n \in \mathbb{P}$. Tällöin

$$\phi(n)\tau(n) = (n-1) \cdot 2 = 2n - 2 = n - 1 + n - 1 = \phi(n) + n - 1$$

ja väitös on osoitettu todeksi. □

Seuraavassa tuloksessa ei esiinny Eulerin $\phi$-funktio lainkaan, mutta sen avulla tuloksen todistaminen on näppärää [5].

**Lause 3.31.** *Kaikilla* $n \geq 2$

$$n + \tau(n) \leq \sigma(n) + 1.$$

*Todistus.* Lauseen 3.5 nojalla $\phi(n) \leq n - 1$, jos $n \geq 2$. Lisäksi lauseen 3.2 perusteella $\sum_{d|n} \phi(d) = n$. Nyt

$$n = \sum_{d|n} \phi(d) = \phi(d_1) + \phi(d_2) + ... + \phi(d_k) \leq 1 + (d_2 - 1) + ... + (d_k - 1).$$

Kun yllä olevaan muotoon lisätään yksi ja vähennetään yksi, saadaan

$$n \leq 1 + \sigma(n) - \tau(n)$$

eli $n + \tau(n) \leq \sigma(n) + 1$. □

**Lause 3.32.** *Kaikille* $n > 1$

$$\phi(n)\sigma(n) < n^2,$$

*ja jos* $n = 1$, *niin* $\phi(n)\sigma(n) = n^2$.

*Todistus.* Oletetaan ensin, että $n \in \mathbb{P}$, jolloin saadaan

$$\phi(n)\sigma(n) = (n-1)(n+1) = n^2 - 1 < n^2$$

eli väitös pätee. Yhtäsuuruus saadaan selvästi, jos $n = 1$. Oletetaan sitten, että $n = p^a$. Tällöin saadaan

$$\phi(n)\sigma(n) = p^{a-1}(p-1)\frac{p^{a+1}-1}{p-1} = p^{a-1}(p^{a+1}-1) = p^{2a} - p^{a-1} < p^{2a}$$

eli tällöinkin väitös pätee. Oletetaan viimeisenä, että $n = \prod_{i=1}^{k} p_i^{a_i}$. Nyt

$$\phi(n)\sigma(n) = \prod_{i=1}^{k} p_i^{a_i-1}(p_i-1)\prod_{i=1}^{k}\frac{p_i^{a_i+1}-1}{p_i-1}$$

ja kun tuloa järjestellään hieman uusiksi sekä supistetaan, saadaan

$$\phi(n)\sigma(n) = \prod_{i=1}^{k} p_i^{a_i-1}(p_i^{a_i+1}-1),$$

missä kukin $p_i^{a_i-1}(p_i^{a_i+1}-1) < p^{2a_i}$. Tästä seuraa, että

$$\phi(n)\sigma(n) < \prod_{i=1}^{k} p_i^{2a_i} = n^2$$

ja lause on täten todistettu. □

Todistetaan seuraavaksi kaksi samankaltaista identiteettiä.

**Lause 3.33.** *Kaikille* $n \geq 1$

$$\sigma(n) = \sum_{d|n} \phi(d)\tau\left(\frac{n}{d}\right).$$

*Todistus.* Olkoon $n = \prod_{i=1}^{k} p_i^{a_i}$. Nyt yhtälössämme esiintyy luvun $n$ jakaja $d$. Merkitään jakajaa $d = p_1^{i_1}p_2^{i_2}\cdots p_k^{i_k}$, missä kukin $0 \leq i_j \leq a_j$, kun $1 \leq j \leq k$. Tarkastellaan yhtälön oikeaa puolta ja saadaan

$$\sum_{d|n} \phi(d)\tau\left(\frac{n}{d}\right) = \sum_{i_1=0}^{a_1}\sum_{i_2=0}^{a_2}\cdots\sum_{i_k=0}^{a_k} \phi(p_1^{i_1}p_2^{i_2}\cdots p_k^{i_k})\tau\left(\frac{n}{p_1^{i_1}p_2^{i_2}\cdots p_k^{i_k}}\right).$$

Koska $\phi$ ja $\tau$ ovat multiplikatiivisia, saadaan oikeasta puolesta edelleen

$$\begin{aligned}
&\sum_{i_1=0}^{a_1}\sum_{i_2=0}^{a_2}\cdots\sum_{i_k=0}^{a_k}\phi(p_1^{i_1})\phi(p_2^{i_2})\cdots\phi(p_k^{i_k})\tau\left(\frac{p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}}{p_1^{i_1}p_2^{i_2}\cdots p_k^{i_k}}\right)\\
=&\sum_{i_1=0}^{a_1}\sum_{i_2=0}^{a_2}\cdots\sum_{i_k=0}^{a_k}\phi(p_1^{i_1})\phi(p_2^{i_2})\cdots\phi(p_k^{i_k})\tau(p_1^{a_1-i_1}p_2^{a_2-i_2}\cdots p_k^{a_k-i_k})\\
=&\sum_{i_1=0}^{a_1}\sum_{i_2=0}^{a_2}\cdots\sum_{i_k=0}^{a_k}\phi(p_1^{i_1})\phi(p_2^{i_2})\cdots\phi(p_k^{i_k})\tau(p_1^{a_1-i_1})\tau(p_2^{a_2-i_2})\cdots\tau(p_k^{a_k-i_k}).
\end{aligned}$$

Koska jokainen summa laskee vain kyseistä indeksiä vastaavat termit, voidaan viimeisin muoto kirjoittaa muotoon

$$\underbrace{\sum_{i_1=0}^{a_1}\phi(p_1^{i_1})\tau(p_1^{a_1-i_1})}_{=A}\sum_{i_2=0}^{a_2}\phi(p_2^{i_2})\tau(p_2^{a_2-i_2})\cdots\sum_{i_k=0}^{a_k}\phi(p_k^{i_k})\tau(p_k^{a_k-i_k}).$$

Merkitköön $A$ yllä olevassa esityksessä yhtä indeksiä vastaavaa summaa. Aletaan purkaa summaa auki ja jätetään indeksit selkeyden vuoksi pois, joten saadaan

$$\begin{aligned}
A &= \phi(1)\tau(p^a)+\phi(p)\tau(p^{a-1})+\phi(p^2)\tau(p^{a-2})+...+\phi(p^{a-1})\tau(p)+\phi(p^a)\tau(1)\\
&= 1\cdot(a+1)+(p-1)(a-1+1)+p(p-1)(a-2+1)+...\\
&\quad +p^{a-2}(p-1)(1+1)+p^{a-1}(p-1)\cdot 1\\
&= a+1+(p-1)(a+p(a-1)+...+2p^{a-2}+p^{a-1}).
\end{aligned}$$

Kerrotaan nyt pitkän sulkulausekkeen sisällä olevat sulut auki ja lisätään termejä selkeyden vuoksi. Kerrotaan sitten sulkujen ulkopuolella oleva yhteinen tekijä $p-1$ takaisin eli saadaan

$$\begin{aligned}
A &= a+1+(p-1)(a+pa-p+p^2a-2p^2+p^3a-3p^3+...+2p^{a-2}+p^{a-1})\\
&= a+1+(\underline{pa}-a+\underline{\underline{p^2a}}-\underline{pa}-p^2+p+\underline{\underline{\underline{p^3a}}}-\underline{\underline{p^2a}}-2p^3+2p^2\\
&\quad +p^4a-\underline{\underline{\underline{p^3a}}}+...+2p^{a-1}-2p^{a-2}+p^a-p^{a-1}).
\end{aligned}$$

Nyt siis sekatermit kumoutuvat pois, jolloin summaamalla samat potenssit,

päästään muotoon

$$\begin{aligned} A &= a + 1 + (-a + p + p^2 + p^3 + ... + p^{a-1} + p^a) \\ &= 1 + p + p^2 + p^3 + ... + p^{a-1} + p^a \\ &= \frac{1 - p^{a+1}}{1 - p} = \frac{p^{a+1} - 1}{p - 1}, \end{aligned}$$

missä keskimmäinen rivi on geometrinen summa, josta viimeinen rivi seuraa. Kun lausekkeen jokainen summa käsitellään vastaavalla tavalla ja indeksit palautetaan, saadaan

$$\begin{aligned} &\sum_{d|n} \phi(d)\tau\left(\frac{n}{d}\right) \\ &= \sum_{i_1=0}^{a_1} \phi(p_1^{i_1})\tau(p_1^{a_1-i_1}) \sum_{i_2=0}^{a_2} \phi(p_2^{i_2})\tau(p_2^{a_2-i_2}) \cdots \sum_{i_k=0}^{a_k} \phi(p_k^{i_k})\tau(p_k^{a_k-i_k}) \\ &= \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{a_k+1} - 1}{p_k - 1} = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}. \end{aligned}$$

Lauseen 2.50 perusteella

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1},$$

joten

$$\sigma(n) = \sum_{d|n} \phi(d)\tau\left(\frac{n}{d}\right).$$

□

Osoitetaan toinen edellisen kaltainen muoto. Todistus noudattelee hyvinkin pitkälti samoja periaatteita.

**Lause 3.34.** *Kaikille* $n \geq 1$

$$n\tau(n) = \sum_{d|n} \phi(d)\sigma\left(\frac{n}{d}\right).$$

*Todistus.* Olkoon $n = \prod_{i=1}^{k} p_i^{a_i}$. Taas yhtälössämme esiintyy luvun $n$ jakaja $d$, jota merkitsemme jälleen $d = p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}$, missä kukin $0 \leq i_j \leq a_j$, kun $1 \leq j \leq k$. Tarkastellaan yhtälön oikeaa puolta ja saadaan funktioiden $\phi$ ja $\sigma$ multiplikatiivisuuden nojalla aivan vastaavasti kuin edellisessä lauseessa

$$\sum_{d|n} \phi(d)\sigma\left(\frac{n}{d}\right) = \underbrace{\sum_{i_1=0}^{a_1} \phi(p_1^{i_1})\sigma(p_1^{a_1-i_1})}_{=A} \sum_{i_2=0}^{a_2} \phi(p_2^{i_2})\sigma(p_2^{a_2-i_2}) \cdots \sum_{i_k=0}^{a_k} \phi(p_k^{i_k})\sigma(p_k^{a_k-i_k}).$$

Merkitköön $A$ yllä olevassa esityksessä yhtä indeksiä vastaavaa summaa vastaavasti kuin edellisessä lauseessa. Lasketaan summa auki jättäen indeksit selkeyden vuoksi pois. Saadaan

$$\begin{aligned}
A &= \phi(1)\sigma(p^a) + \phi(p)\sigma(p^{a-1}) + \phi(p^2)\sigma(p^{a-2}) + ... + \phi(p^{a-1})\sigma(p) + \phi(p^a)\sigma(1) \\
&= \frac{p^{a+1}-1}{p-1} + (p-1)\frac{p^a-1}{p-1} + p(p-1)\frac{p^{a-1}-1}{p-1} + ... \\
&\quad + p^{a-2}(p-1)(p+1) + p^{a-1}(p-1) \\
&= \frac{p^{a+1}-1}{p-1} + (p^a-1) + (p^a-p) + (p^a-p^2) + ... \\
&\quad + (p^a-p^{a-2}) + (p^a-p^{a-1}).
\end{aligned}$$

Lisätään ja vähennetään luku $p^a$, jolloin saadaan

$$\begin{aligned}
A &= \frac{p^{a+1}-1}{p-1} + (p^a-1) + (p^a-p) + (p^a-p^2) + ... \\
&\quad + (p^a-p^{a-2}) + (p^a-p^{a-1}) + (p^a-p^a) \\
&= \frac{p^{a+1}-1}{p-1} + (a+1)p^a - (1+p+p^2+...+p^{a-1}+p^a) \\
&= \frac{p^{a+1}-1}{p-1} + (a+1)p^a - \frac{p^{a+1}-1}{p-1} = (a+1)p^a.
\end{aligned}$$

Kun jokainen summa käsitellään vastaavalla tavalla, voidaan summat tämän

jälkeen kertoa eli

$$\begin{aligned}
&\sum_{d|n} \phi(d)\sigma\left(\frac{n}{d}\right) \\
&= \sum_{i_1=0}^{a_1} \phi(p_1^{i_1})\sigma(p_1^{a_1-i_1}) \sum_{i_2=0}^{a_2} \phi(p_2^{i_2})\sigma(p_2^{a_2-i_2}) \cdots \sum_{i_k=0}^{a_k} \phi(p_k^{i_k})\sigma(p_k^{a_k-i_k}) \\
&= (a_1+1)p_1^{a_1}(a_2+1)p_2^{a_2}\cdots(a_k+1)p_k^{a_k} \\
&= p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}(a_1+1)(a_2+1)\cdots(a_k+1) = \prod_{i=1}^{k} p_i^{a_i} \prod_{i=1}^{k}(a_i+1) \\
&= n\tau(n)
\end{aligned}$$

ja lause on täten todistettu. □

Aiemmin osoitettiin, että $n$ on alkuluku, jos ja vain jos $\phi(n) = n - 1$. Osoitetaan nyt toinen riittävä ehto (ks. esim. [10, s. 169]).

**Lause 3.35.** *Jos $n \in \mathbb{P}$, niin $\sigma(n) + \phi(n) = n\tau(n)$. Käänteisesti, jos $\sigma(n) + \phi(n) = n\tau(n)$, niin $n \in \mathbb{P}$.*

*Todistus.* Oletetaan ensin, että $n \in \mathbb{P}$. Tällöin

$$\sigma(n) + \phi(n) = (n+1) + (n-1) = 2n = n(1+1) = n\tau(n)$$

eli ensimmäinen vaihe on todistettu. Oletetaan sitten, että on voimassa $\sigma(n) + \phi(n) = n\tau(n)$. Tällöin pitää olla $n > 1$, koska jos $n = 1$, niin yhtälö ei selvästikään päde. Tehdään sitten vastaoletus, että $n$ ei ole alkuluku vaan $n = \prod_{i=1}^{k} p_i^{a_i}$. Nyt lauseen 3.34 perusteella pitää olla

$$\sigma(n) + \phi(n) = \sum_{d|n} \phi(d)\sigma\left(\frac{n}{d}\right).$$

Kun lasketaan auki yhtälön oikea puoli, saadaan

$$\sum_{d|n} \phi(d)\sigma\left(\frac{n}{d}\right) = \sum_{d|p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}} \phi(d)\sigma\left(\frac{p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}}{d}\right)$$

$$= \phi(1)\sigma(p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}) + \phi(p_1)\sigma(p_1^{a_1-1}p_2^{a_2}\cdots p_k^{a_k}) + \phi(p_1^2)\sigma(p_1^{a_1-2}p_2^{a_2}\cdots p_k^{a_k})$$
$$+ ... + \phi(p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k-1})\sigma(p_k) + \phi(p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k})\sigma(1)$$

$$= \sigma(p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}) + \phi(p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k})$$
$$+ \phi(p_1)\sigma(p_1^{a_1-1}p_2^{a_2}\cdots p_k^{a_k}) + \phi(p_1^2)\sigma(p_1^{a_1-2}p_2^{a_2}\cdots p_k^{a_k}) + ...$$
$$+ \phi(p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k-1})\sigma(p_k).$$

Nyt siis pitäisi olla $\phi(p_1)\sigma(p_1^{a_1-1}p_2^{a_2}\cdots p_k^{a_k}) + \phi(p_1^2)\sigma(p_1^{a_1-2}p_2^{a_2}\cdots p_k^{a_k}) + ... + \phi(p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k-1})\sigma(p_k) = 0$, mikä on ristiriita, koska $\phi(n), \sigma(n) > 0$ kaikilla $n > 0$. Pitää siis olla $n \in \mathbb{P}$. □

# Viitteet


[1] Dineva R., *The Euler Totient, the Möbius and the Divisor Functions.* Mount Holyoke College. 2005. Saatavilla <http://www.mtholyoke.edu/~robinson/reu/reu05/rdineva1.pdf> 12.11.2013

[2] *GIMPS – Great Internet Mersenne Prime Search.* <http://www.mersenne.org/default.php> 12.11.2013.

[3] Haukkanen P., *Lukuteoriaa.* Opetusmoniste. Tampereen yliopisto.

[4] *MathWorld – A Wolfram Web Resource.* <http://mathworld.wolfram.com/> 12.11.2013.

[5] Minculete N., Dicu P., *Concerning the Euler totient.* General Mathematics Vol. 16, No. 1, 93-99. 2008. Saatavilla <http://www.emis.de/journals/GM/vol16nr1/dicu/dicu.pdf> 12.11.2013

[6] Rosen K. H., *Elementary Number Theory – and Its Applications.* Sixth Edition. Pearson. 2011.

[7] Sándor J., *Geometric Theorems, Diophantine Equations, And Arithmetic Functions* American Research Press. Rehoboth. 2002.

[8] Sándor J., Crstici B., *Handbook of Number Theory II.* Kluwer Academic Publishers. 2004.

[9] Sivaramakrishnan R., *Classical Theory of Arithmetic Functions.* Marcel Dekker Inc. 1989.

[10] Tattersall J. J., *Elementary Number Theory in Nine Chapters.* Cambridge University Press. 1999.